Linux Association of Canada

LINUX ASSOCIATION OF CANADA PUBLIC GUIDE

CYBERSECURITY FUNDAMENTALS

FOR SMALL ORGANIZATIONS

Protecting People, Information and Essential Services

SIMPLE STEPS
Practical actions any organization can take

STRONGER TOGETHER
Build a culture of security every day

PROTECT WHAT MATTERS
Keep your people, data and services safe

CANADIAN FOCUS
Resources and guidance for organizations in Canada

linuxassociation.ca | info@linuxassociation.ca | (639) 477-0111

Contents

PART ONE

Understanding Cybersecurity

Why it matters, who this guide is for, and today's threat landscape

About This Guide

Why Cybersecurity Matters

Cybersecurity is no longer optional or reserved for large enterprises and government agencies. For small and medium-sized organizations across Canada—professional services firms, healthcare clinics, non-profits, manufacturers, and community organizations—cybersecurity has become fundamental to operational continuity, client trust, and organizational reputation.

A single security incident can disrupt operations for days or weeks, compromise sensitive client or employee information, trigger regulatory obligations, damage relationships built over years, and impose financial costs many small organizations struggle to absorb. The Canadian Centre for Cyber Security reports that cyber threats have increased in frequency and sophistication, with small organizations facing the same threat landscape as larger counterparts but with fewer resources to respond.

The business impact extends beyond technical disruption: legal liability, regulatory penalties, notification requirements, credit monitoring obligations, and reputational damage affecting client acquisition and retention. Insurance premiums may rise, and partners increasingly require evidence of security practices before doing business.

Yet cybersecurity is fundamentally about people, processes, and informed decision-making, not expensive tools. The most effective measures are often the simplest: strong authentication, regular backups, software updates, employee awareness, and clear procedures. This guide approaches cybersecurity as an organizational capability that protects your people, safeguards your information, maintains your ability to deliver services, and strengthens your position in your community and industry.

Who This Guide Is For

This guide is designed for small and medium-sized Canadian organizations—typically fewer than 100 employees—across all sectors, including those without dedicated IT staff or substantial technology budgets.

- Executive leadership and decision makers: strategic context for security investments and building organizational security culture
- Administrative and operational staff: practical guidance for daily responsibilities as a first line of defense
- Finance and accounting professionals: risks related to financial fraud, business email compromise, and payment security
- Human resources personnel: protecting employee information and secure onboarding/offboarding
- Client-facing staff: protecting client information and recognizing social engineering
- Technical staff and IT coordinators: framework for communicating priorities to non-technical colleagues
- Board members and volunteers: governance responsibilities related to cybersecurity

No specialized technical knowledge is assumed. Terms are explained in plain language, and

recommendations are practical and achievable within typical small-organization constraints.

How to Use This Guide

This guide works as a comprehensive introduction read sequentially, a reference resource consulted by topic, a planning tool with assessment frameworks and roadmaps, an educational resource for staff training, and a foundation for policy development.

Throughout, you will find clear explanations in plain language, practical examples relevant to small organizations, actionable recommendations, risk context for prioritization, and a Canadian perspective reflecting our regulatory environment and threat landscape. The guide emphasizes achievable progress over perfect security—meaningful risk reduction through practical, sustainable measures.

Security Is Everyone's Responsibility

Cybersecurity is not solely an IT responsibility—it is organizational, extending to every role. Technical measures like firewalls and antivirus cannot defend against every threat; many successful attacks exploit human factors, such as an employee clicking a malicious link or a manager approving a fraudulent payment.

Conversely, security-aware individuals across the organization create multiple layers of defense. This distributed responsibility does not require everyone to become a security expert—it means everyone understands basic principles relevant to their role, recognizes common threats, knows how to respond to suspicious situations, and feels empowered to report concerns without fear of blame.

Building this culture requires leadership commitment, clear communication, practical training, and recognition that security measures must be realistic and sustainable. Effective security integrates into daily work rather than creating obstacles to it.

What Is Cybersecurity?

Cybersecurity encompasses the practices, technologies, and processes that protect digital information, computer systems, networks, and services from unauthorized access, damage, disruption, or misuse. At its foundation is the CIA Triad: Confidentiality, Integrity, and Availability—a framework for understanding security objectives that every security decision ultimately serves.

Confidentiality: Protecting Information from Unauthorized Access

Confidentiality ensures information is accessible only to those authorized to view or use it. This applies to client and customer information, employee information, financial information, business information, and authentication credentials.

Breaches can result from cyberattacks, employees accessing information beyond their role, lost or stolen unencrypted devices, misdirected emails, or improper disposal of materials. Protecting confidentiality requires access controls, encryption, secure communication channels, proper authentication, and employee training. The business impact includes regulatory penalties, notification obligations, legal liability, and loss of client trust.

Integrity: Ensuring Information Accuracy and Trustworthiness

Integrity ensures information remains accurate, complete, and unaltered except through authorized processes—protecting against unauthorized modification, corruption, or deletion. This matters for financial records, client records, contracts, system configurations, and audit trails.

Integrity threats include malware that modifies files, attackers who alter data for fraud, system errors, and accidental modifications. Protection requires access controls, audit logging, backup systems, validation processes, and separation of duties. Unlike confidentiality breaches, integrity compromises may go undetected for extended periods.

Availability: Ensuring Access When Needed

Availability ensures information, systems, and services remain accessible to authorized users when needed—protecting against disruptions from technical failures, cyberattacks, natural disasters, or other causes. This is essential for email, financial systems, client-facing systems, and collaboration tools.

Threats include ransomware, distributed denial-of-service attacks, hardware failures, power outages, and human error. Protection requires robust backups, redundant systems, disaster recovery planning, capacity planning, and incident response procedures. The business impact of extended outages can include lost revenue, client defection, and reputational damage.

The Interplay of Confidentiality, Integrity, and Availability

These principles are interconnected and sometimes in tension: encryption protects confidentiality but may impact availability if keys are lost; access restrictions protect confidentiality and integrity but may reduce availability if too restrictive; backups protect availability and integrity but create copies that must be secured for confidentiality; audit logging supports integrity but creates logs that must be protected for confidentiality.

For small organizations, the CIA Triad provides a practical framework for evaluating security decisions: does this measure protect confidentiality, integrity, or availability, does it create tensions with other goals, and is the protection proportionate to the risk?

Why Small Organizations Are Targets

A persistent, dangerous misconception among small organizations is that their size provides protection from cyber threats. The reality is considerably different: attackers do not care how small you are.

The Economics of Automated Attacks

Modern cyberattacks are largely automated, conducted by tools that scan the internet continuously, probing millions of systems for vulnerabilities without regard to organization size or profile. An attacker can deploy automated tools attempting to compromise thousands of organizations simultaneously at minimal cost. Obscurity provides no protection—you simply need to be connected to the internet with an exploitable vulnerability.

Why Small Organizations Are Attractive Targets

- Lower security defenses – fewer resources, less sophisticated infrastructure, less expertise, making compromise easier
- Less security awareness – employees may receive less training, increasing phishing and social engineering success rates
- Valuable information despite size – client lists, financial information, employee data, and credentials all have value
- Access to larger organizations – small organizations serve as entry points to larger partners through supply chain attacks
- Lower detection likelihood – lack of sophisticated monitoring means compromises can go undetected for extended periods
- Higher payment likelihood – in ransomware attacks, small organizations may be more likely to pay due to lack of backups or insurance

Common Threats Facing Small Organizations

Ransomware has become one of the most significant threats, encrypting files and systems and demanding payment. The impact can be devastating, and a significant percentage of small businesses that experience major ransomware attacks without adequate backups never fully recover.

Phishing remains the most common attack vector, using fraudulent emails, texts, or websites to trick recipients into revealing passwords or transferring money. Small organizations are particularly vulnerable due to less familiarity with sophisticated techniques.

Business Email Compromise (BEC) involves attackers impersonating executives, vendors, or partners after extensive reconnaissance, tricking employees into transferring funds. Organizations have lost hundreds of thousands of dollars to single BEC attacks.

Financial fraud encompasses fraudulent invoices, payment information manipulation, credit card theft, unauthorized bank access, and payroll fraud. Identity theft targeting employees or the organization can result in fraudulent credit applications, tax fraud, and reputational damage.

The Reality: Size Provides No Protection

The question is not whether your organization will face cyber threats—you already do, continuously—but whether you have implemented basic protections that significantly reduce your risk. Many effective security measures are not expensive or complex; they require awareness, consistent practices, and organizational commitment. Small organizations that implement fundamental practices become harder targets, and attackers often move on to more vulnerable victims.

Understanding Today's Threat Landscape

Effective cybersecurity requires understanding where threats originate, what motivates them, and how they manifest. Threats come from multiple sources, each with different motivations, capabilities, and methods.

Cyber Criminals: Financially Motivated Attackers

Cyber crime has become a sophisticated global industry with specialized roles and professional operations. Ransomware operations often function as businesses with customer service and affiliate programs. Data theft operations steal and monetize sensitive information through underground marketplaces. BEC specialists conduct extensive reconnaissance and execute sophisticated fraud. Cryptojacking operations compromise systems to mine cryptocurrency without consent.

Insider Threats: Risks from Within

Insider threats originate from employees, contractors, volunteers, or partners with authorized access. Malicious insiders deliberately harm the organization through theft, sabotage, or fraud. Negligent insiders cause harm through carelessness without malicious intent. Compromised insiders are legitimate users whose credentials have been stolen by external attackers. Effective mitigation requires access controls, activity monitoring, security awareness, and a culture encouraging reporting.

Human Error: Unintentional Security Failures

Well-intentioned employees make mistakes that create vulnerabilities: misconfiguration of systems, accidental disclosure through misdirected emails, lost or stolen unencrypted devices, falling victim to sophisticated social engineering, or failure to follow procedures due to time pressure. Human error can be significantly reduced through clear policies, practical procedures, regular training, and technical controls that make secure actions the default.

Natural Disasters and Environmental Threats

Severe weather, fires, power failures, and infrastructure failures can disrupt operations, damage systems, and compromise availability. Organizations without robust backups or business continuity procedures may experience extended outages. The increasing frequency of extreme weather due to climate change makes environmental planning increasingly important.

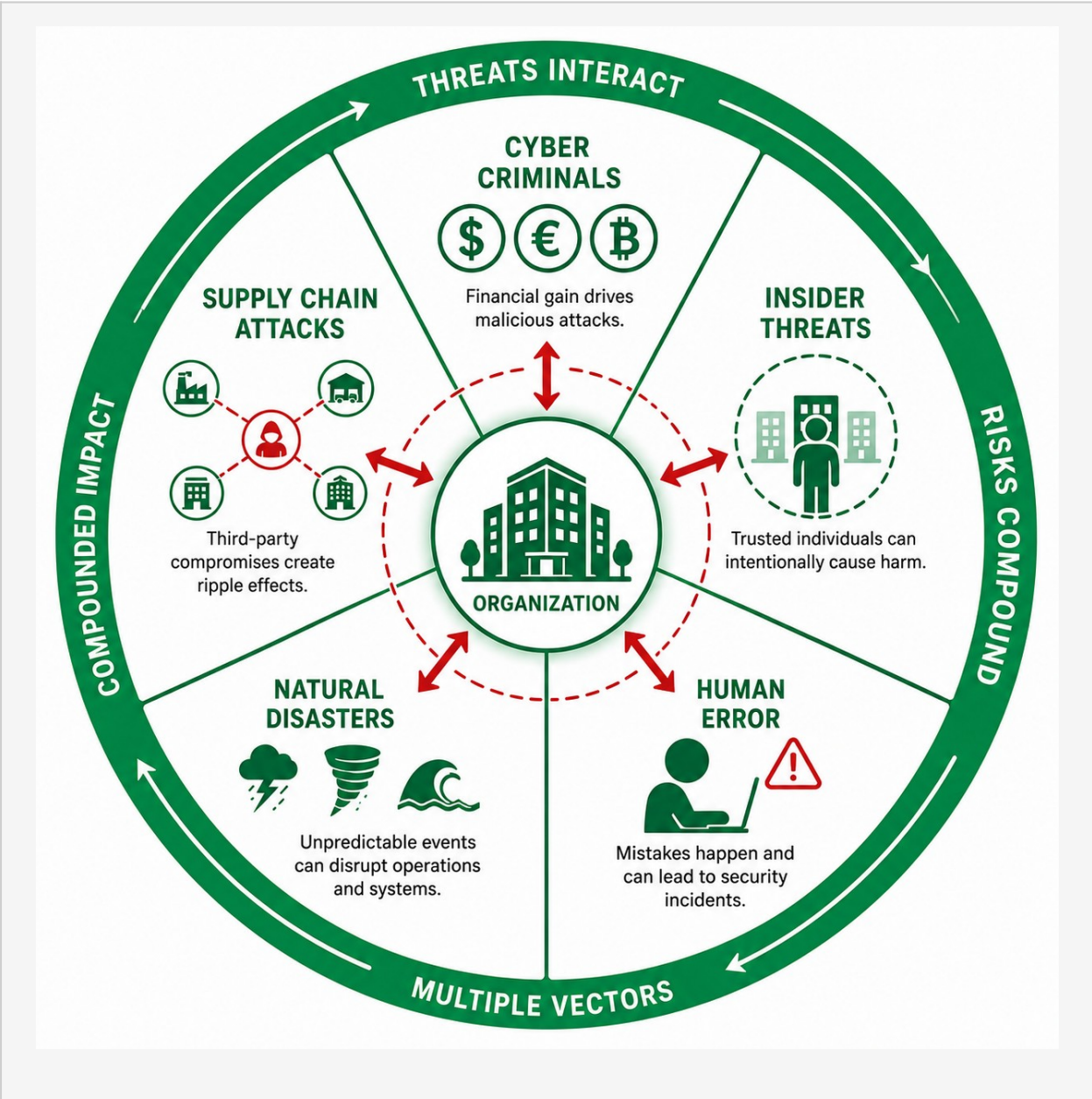
Supply Chain Attacks: Compromise Through Trusted Relationships

Attackers compromise vendors, suppliers, or software providers and use that access to reach their ultimate target, exploiting trust relationships. This includes vendor compromise, software supply chain attacks, hardware supply chain attacks, and service provider compromise. Defending requires careful vendor selection, contractual security requirements, and monitoring of vendor access.

The Interconnected Nature of Threats

These categories interact and compound each other: cyber criminals exploit human error through

phishing; insider threats may be financially motivated; natural disasters create opportunities for criminals targeting disrupted organizations; supply chain compromises enable criminals to bypass direct defenses. Comprehensive security strategies must address multiple threat vectors rather than focusing narrowly on single threat types.



Building a Security Culture

The most sophisticated security technologies will fail if organizational culture does not support security. Organizations with strong security cultures achieve significant protection even with modest technical resources.

Cybersecurity Is Not Just an IT Problem

A fundamental misconception is that cybersecurity is solely IT's responsibility. Most security risks involve human decisions across all functions: an employee clicking a phishing link, a staff member approving a fraudulent payment, a manager leaving documents visible. Technical measures reduce these risks but cannot eliminate them—human judgment remains essential.

Security Responsibilities Across Organizational Roles

Reception and front-desk staff

Verify visitor identities, recognize suspicious phone calls, follow sign-in procedures, protect visible sensitive information, and recognize social engineering attempts.

Finance and accounting personnel

Verify payment requests through independent channels, recognize BEC and invoice fraud, protect financial information, follow separation-of-duties procedures, and report anomalies.

Human resources personnel

Protect employee personal information, implement secure onboarding and offboarding, recognize fraudulent applications, and maintain confidentiality of personnel matters.

Management and leadership

Demonstrate commitment through their own practices, allocate resources, support policies even when inconvenient, foster blame-free reporting culture, and hold personnel accountable.

Volunteers and temporary staff

Follow the same policies as permanent staff, receive appropriate training before accessing systems, and understand access will be limited based on role and duration.

All staff

Use strong unique passwords, recognize and report phishing, keep software updated, protect mobile devices, follow clean desk policies, and report incidents promptly.

Creating a Culture Where Security Is Everyone's Responsibility

- Leadership commitment – visible support, resource allocation, consistent messaging
- Clear communication – plain language, not technical jargon buried in lengthy documents
- Practical, realistic policies – balance security with operational needs
- Regular training and awareness – not just one-time onboarding training
- Positive reinforcement – recognize and reward good security practices
- Blame-free incident reporting – encourage reporting mistakes without fear of punishment
- Integration into daily operations – security as a natural part of work, not an added burden

- Continuous improvement – based on lessons learned and changing threats

Building a security culture is a long-term effort requiring patience, consistency, and commitment. Organizations with strong security cultures achieve significantly better outcomes than those relying solely on technical measures.

PART TWO

Protecting Your Information

Your most valuable asset, and how to classify it

Your Most Valuable Asset: Information

Organizations often focus security efforts on physical assets, but these are merely containers for what truly matters: information. Your organization's most valuable assets are not the hardware you own, but the information you create, collect, process, and store.

Customer and Client Data

Contact information, transaction history, financial information, personal identifiers, health information, and behavioral data are entrusted to your organization. Unauthorized disclosure can result in regulatory penalties, legal liability, notification obligations, and loss of customer trust.

Employee Files and Personnel Information

Personal information, financial information, employment history, health and benefits information, and time and attendance records. Employees expect this to remain private; breaches can result in identity theft, legal liability, and damage to employee trust.

Financial Records and Accounting Information

Banking information, accounts receivable/payable, payroll, financial statements, tax records, and contracts. Unauthorized access can enable fraud or reveal information that damages negotiating positions.

Passwords and Authentication Credentials

User account credentials, administrative credentials, service account credentials, encryption keys, and API keys control access to other information and systems. Credential theft is a primary objective of many cyberattacks because credentials provide ongoing access.

Email and Communications

Business communications, sensitive discussions, attachments, and metadata. Email compromise can expose years of communications and provide attackers with intelligence for further attacks.

Contracts, Agreements, and Legal Documents

Customer contracts, vendor agreements, employment agreements, leases, intellectual property documents, and legal correspondence. Unauthorized access can reveal confidential terms and provide competitors with strategic intelligence.

The Business Value of Information

Understanding value helps prioritize protection: replacement cost (some information cannot be recreated at any cost), competitive value, regulatory obligations, reputational impact, and operational criticality. By understanding what you hold, why it is valuable, and what harm could result from its compromise, you can make informed decisions about appropriate protection measures.


CONTRACT
*****
INFORMATION

Information Classification

Not all information requires the same level of protection. A public press release does not require the same security measures as employee salary information. Information classification provides a systematic framework for applying appropriate protection to each category, focusing security resources on what matters most.

The Four-Level Classification Framework

Public

Intended for unrestricted disclosure: marketing materials, public website content, press releases, published financial statements, job postings. Requires minimal protection—mainly maintaining integrity. Can be shared freely and posted publicly.

Internal

Intended for use within the organization but not public disclosure: internal policies, meeting agendas, organizational charts, routine operational information. Requires basic access controls limiting access to employees and authorized partners; should not be posted publicly.

Confidential

Sensitive business information that could cause significant harm if disclosed: customer and employee personal information, detailed financial statements, business strategy, pricing, vendor agreements, security policies, legal documents.

Requires: access limited to legitimate business need, encryption in storage and transit, secure disposal, clear labeling, access logging, and confidentiality agreements. Should not be discussed in public spaces or unsecured channels.

Highly Sensitive

The most sensitive information held: authentication credentials, credit card and banking credentials, social insurance numbers, protected health information, trade secrets, legal privileged communications, executive strategic information, encryption keys.

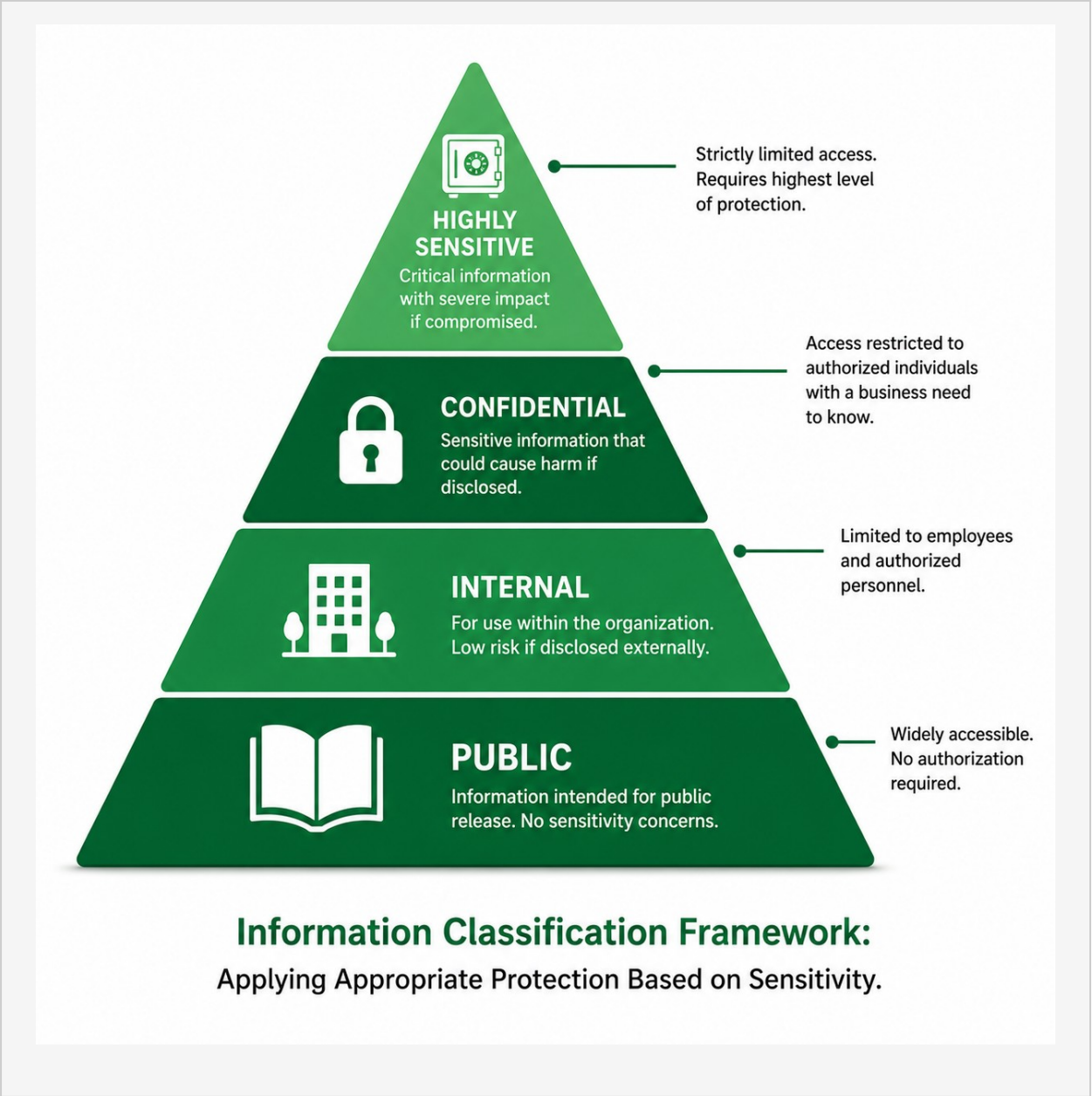
Requires: strictly limited access on a need-to-know basis, strong encryption, multi-factor authentication, comprehensive audit logging, strict handling procedures, regular access reviews, and immediate notification if compromised.

Applying Classification in Practice

- Classification at creation – information classified when created or received
- Clear labeling – headers, footers, subject lines, or physical stamps indicating classification
- Default to higher classification when in doubt
- Periodic classification review – information classification changes over time
- Declassification when protection is no longer needed
- Training – all employees understand the framework and how to handle each level

Benefits of Information Classification

Focused protection on the most sensitive information, clear expectations reducing confusion, support for regulatory compliance, informed risk-based decisions, and efficient operations by avoiding over-protection of non-sensitive information. Classification is about applying appropriate protection based on sensitivity and value, enabling both effective security and efficient operations.



PART THREE

Identity and Access

Strong passwords, password managers, and multi-factor authentication

Strong Passwords

Passwords remain the primary authentication method for most systems. The quality of your passwords directly determines how easily attackers can compromise your accounts—weak passwords can be cracked in seconds; strong passwords can resist attack for years.

Why Password Security Matters

Attackers obtain passwords through brute force attacks (trying every combination), dictionary attacks (common words and known breached passwords), credential stuffing (reusing breached username/password pairs across services), and phishing/social engineering.

The Four Pillars of Password Strength

Length: The Most Important Factor

Each additional character exponentially increases possible combinations. Minimum length recommendations: 12 characters absolute minimum, 14-16 recommended for most accounts, 20+ for highly sensitive and administrative accounts. Eight-character passwords, even complex ones, can be cracked relatively quickly and should no longer be considered adequate.

Complexity: Increasing the Character Space

Mixing lowercase, uppercase, numbers, and symbols increases possible combinations, but complexity alone does not create strong passwords—a complex short password is weaker than a longer, simpler one. Avoid predictable substitutions ("@" for "a") that attackers specifically test. Prioritize length first.

Uniqueness: Never Reuse Passwords

Every account should have a unique password. Password reuse allows a single compromised password to provide access to multiple accounts, and attackers exploit this through credential stuffing. This is why password managers are essential—they enable uniqueness without requiring human memory.

Memorability: Passphrases as a Solution

Passphrases—sequences of random words or meaningful phrases—achieve both strength and memorability. Examples: "CorrectHorseBatteryStaple", "Coffee-Morning-Bicycle-Garden", "I love hiking in Banff National Park". A four-word passphrase of 16-20 characters is significantly stronger than an 8-character complex password and far easier to remember.

Good vs. Poor Password Examples

Poor passwords (never use these patterns):

- "password" or "Password123" – common, cracked instantly
- "john2024" – names with years are easily guessed
- "Qwerty123!" – keyboard patterns provide no real security
- "Welcome1!" – common corporate password patterns are specifically targeted
- "P@ssw0rd" – predictable substitutions do not significantly increase security

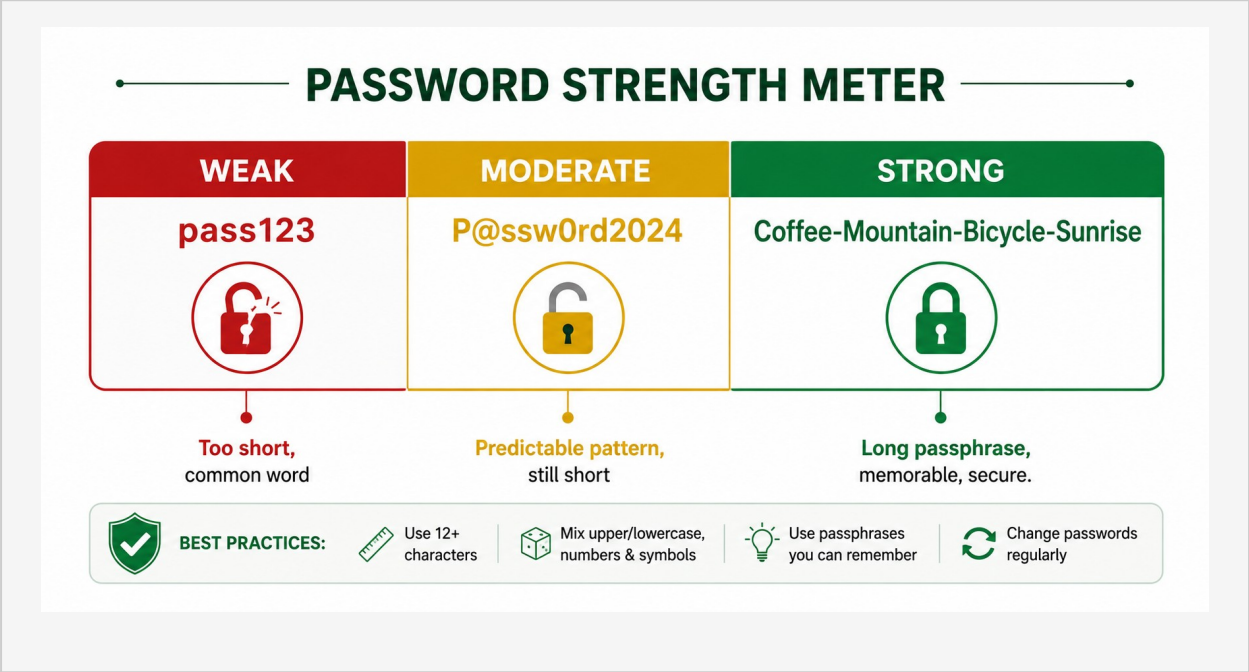
Good passwords and passphrases:

- "Tr0ut-F1shing-Morn1ng-C0ffee" – 31 characters, memorable, extremely strong
- "MyDog&CatLove2PlayInTheGarden!" – 34 characters, memorable, very strong
- "Coffee.Bicycle.Mountain.Sunset.Ocean" – 37 characters, memorable pattern, extremely strong

Implementing Strong Password Practices

- Establish clear policies specifying minimum length (12+) and encouraging passphrases
- Provide training explaining why password security matters
- Implement technical controls: strength meters, rejection of commonly compromised passwords
- Deploy password managers to eliminate memorization burden
- Require password updates only when compromise is suspected, not on arbitrary schedules
- Lead by example – leadership must demonstrate strong password practices

Strong passwords cost nothing to implement and provide immediate security benefits. Every organization can implement strong password practices today.



Password Managers

Strong, unique passwords for every account create a practical challenge: remembering dozens of them. The answer is that you don't need to. Password managers securely store and manage passwords, enabling strong, unique passwords everywhere while you only remember one master password.

Why Password Managers Matter

A typical employee needs 20-30+ passwords across email, CRM, accounting, cloud storage, banking, and more. Expecting anyone to remember that many unique strong passwords is unrealistic—the inevitable result is reuse, weak passwords, or written passwords. Password managers eliminate the memorization burden, enable true uniqueness, facilitate strength through generated random passwords, reduce friction, improve productivity, and provide secure sharing for shared accounts.

How Password Managers Work

Password managers store passwords in an encrypted "vault" protected by a master password only you know. You create the master password, the manager creates an encrypted vault, you add passwords (often automatically captured), the manager fills passwords automatically, and your vault syncs across devices. Critically, encryption and decryption happen on your device using "zero-knowledge" architecture—the provider cannot access your passwords even if their servers are compromised.

Benefits Beyond Password Storage

- Password generation – instantly create strong, random passwords of any length
- Security auditing – identifies weak, reused, or breached passwords
- Secure notes – store security questions, license keys, Wi-Fi passwords
- Secure sharing – share passwords with colleagues without insecure channels
- Emergency access – designated individuals can access your vault after a waiting period
- Breach monitoring – alerts if stored credentials appear in known breaches

Choosing a Password Manager

Consider security and encryption (AES-256, zero-knowledge, independent audits), ease of use, cross-platform support, organizational features (team sharing, admin controls), reliability, and cost.

Popular reputable options:

- Bitwarden – open-source, excellent security, free for individuals, affordable business plans
- 1Password – user-friendly, strong business features
- LastPass – established provider, free and paid tiers
- KeePass/KeePassXC – free, open-source, local storage, more technical setup
- Dashlane – user-friendly, includes VPN in some plans

For small organizations, Bitwarden and 1Password are frequently recommended for their

combination of security, usability, and reasonable cost.

Implementing Password Managers in Your Organization

- Select an appropriate solution based on needs, capabilities, and budget
- Develop clear policies about master password strength and shared passwords
- Provide training on installation, configuration, and daily use
- Lead by example – management adopts first
- Migrate gradually – start with new accounts
- Provide ongoing support and address skepticism about storing passwords in one place

The Master Password: Your Single Point of Security

Minimum 20 characters, preferably 25-30, a memorable passphrase, never reused elsewhere, memorized without writing down for regular use, but written down and stored securely (safe, safety deposit box) for emergency access. Password managers transform password security from an impossible burden into a manageable practice.

Multi-Factor Authentication

Passwords have a fundamental limitation: they are a single factor. If an attacker obtains your password, they can access your account. Multi-factor authentication (MFA) requires two or more independent types of evidence to verify identity, so a stolen password alone is not enough. According to Microsoft research, MFA blocks over 99.9% of account compromise attacks.

The Three Authentication Factors

Something you know

A password, PIN, or security question—the traditional method, but weak alone because knowledge can be transferred once stolen.

Something you have

A physical object: smartphone authentication apps (Google/Microsoft Authenticator, Authy) generating time-based codes; SMS text messages (weakest MFA method, vulnerable to SIM-swapping); hardware security keys (YubiKey, Titan) which are the strongest and cannot be phished; push notifications approved directly on your phone.

Something you are

Biometric characteristics—fingerprints, facial recognition, iris scans. Increasingly common on smartphones and laptops as a convenience factor for device unlock.

How Multi-Factor Authentication Protects You

Against phishing, an attacker who steals your password still lacks your second factor. Against data breaches, stolen passwords alone cannot access accounts with MFA. Against keyloggers, malware can capture keystrokes but not a one-time code or physical key. The security improvement is dramatic—attackers face the additional challenge of obtaining your physical device.

Implementing Multi-Factor Authentication

Prioritize critical accounts:

- Email accounts (often enable password resets for other accounts)
- Financial and banking accounts
- Administrative accounts for business systems
- Cloud storage and backup services
- Customer relationship management and accounting/payroll systems

Choose the strongest supported method (in order of strength):

- Hardware security keys (strongest, most phishing-resistant)
- Authentication apps (strong, convenient, widely supported)
- Push notifications (convenient, reasonably secure)
- SMS text messages (weakest, but better than no MFA)

Establish backup authentication methods and secure backup codes in your password manager. Train employees on setup, lost-device procedures, and recognizing MFA-related phishing.

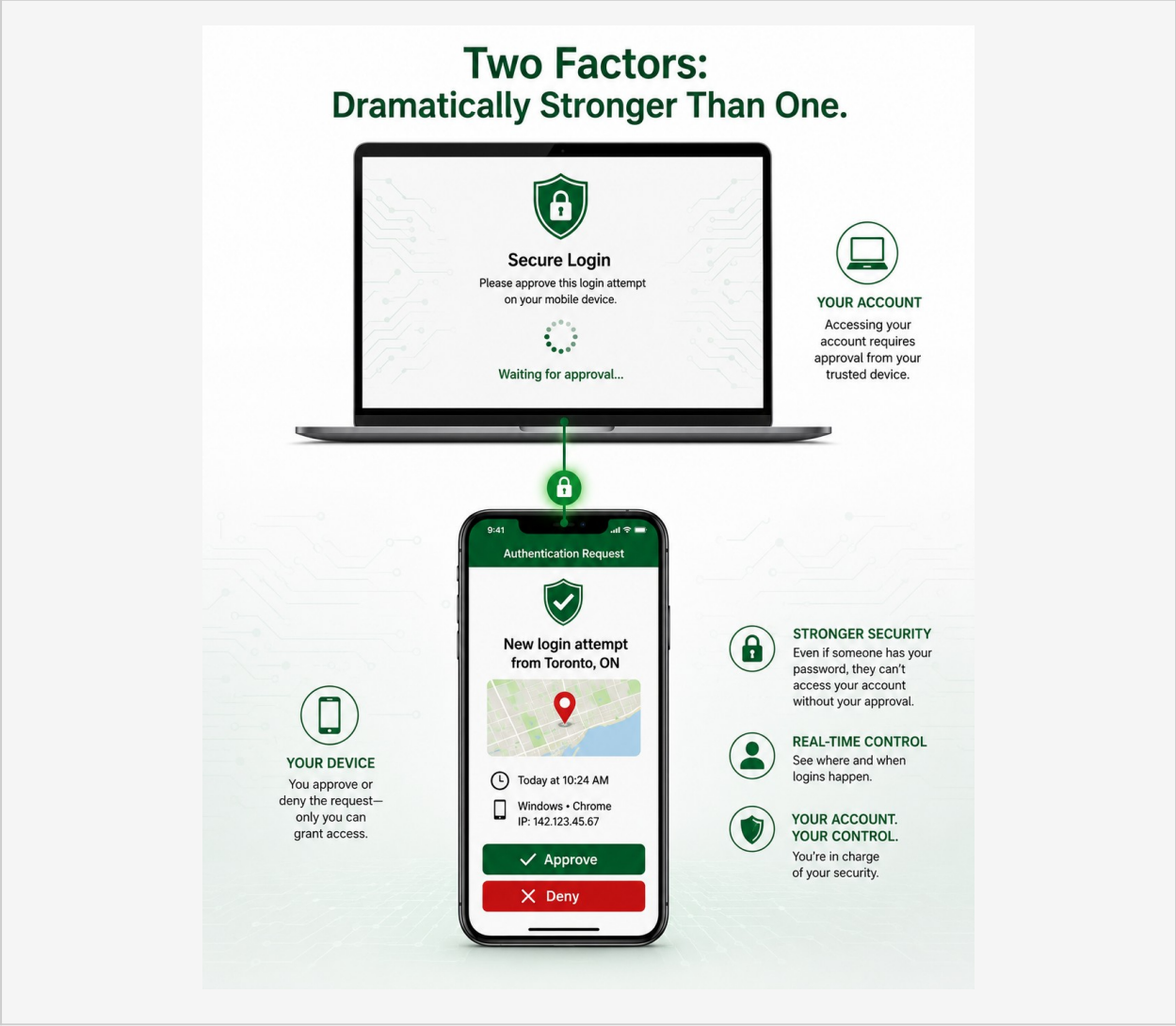
MFA and Organizational Policy

Mandate MFA for critical accounts (non-negotiable for admin, financial, email); recommend it for all accounts; specify approved methods (authentication apps or hardware keys over SMS for sensitive accounts); establish device management and lost-device procedures.

Common MFA Misconceptions

MFA adds only seconds to login, is straightforward for non-technical users, is inexpensive (apps are free, hardware keys $20-50 lasting years), and while not absolute protection, dramatically improves security. SMS is the weakest method and should be replaced by authentication apps or hardware keys where possible.

If you implement only one security measure from this guide, make it multi-factor authentication for all critical accounts.



PART FOUR

Email and Social Threats

Email security, phishing recognition, and social engineering

Email Security

Email remains the primary communication channel for most organizations and, consequently, the primary attack vector for cyber criminals, used to deliver malware, conduct phishing, commit fraud, and gain initial access.

Why Email Is So Vulnerable

Email protocols were designed for convenience, not security: sender addresses can be forged, standard email has no built-in encryption, attachments can carry malware, links can be disguised, and the volume of email creates conditions for quick decisions without scrutiny.

Business Email Compromise: The Most Costly Email Threat

BEC is sophisticated fraud where attackers impersonate executives, vendors, or partners to trick employees into transferring money. Attacks typically follow: reconnaissance (studying org charts, relationships), impersonation (similar domain names, matching display names), social engineering (exploiting authority, urgency, trust—CEO fraud, vendor invoice fraud, attorney impersonation, payroll diversion), and exploitation.

Example: an email from "CEO@company.co" (note the .co) to the Finance Director requesting an urgent, confidential wire transfer while the CEO is "unavailable by phone." This exploits authority, urgency, and confidentiality to discourage verification.

Defending against BEC:

- Mandatory verification procedures for all payment requests via a separate channel
- Dual authorization for wire transfers and significant payments
- Scrutinize sender email addresses, not just display names
- Question urgency and confidentiality requests
- Document standard payment procedures and require verification for deviations

Fake Invoice and Payment Fraud

Fake invoices for services never provided, invoice modification redirecting payments, and vendor impersonation. Defend by maintaining a verified vendor list, verifying invoices against purchase orders, and confirming payment changes through separate channels.

Account Verification and Password Reset Scams

Emails claiming to be from banks or services requesting account verification or password resets, exploiting fear and urgency. Never click links in unsolicited emails—navigate directly to services instead.

Email Security Best Practices

Technical controls:

Email filtering, sender authentication (SPF, DKIM, DMARC), link and attachment scanning, and encryption for sensitive communications.

User practices:

Scrutinize unexpected emails, verify sender identity, hover before clicking, be cautious with attachments, question urgency, and use separate channels for verification.

Organizational procedures:

Mandatory verification for financial transactions, blame-free reporting mechanisms, regular training and simulated exercises, and clear incident response procedures. Email security is primarily a human challenge—technical controls provide important protection but employee awareness and verification procedures are essential.

Recognizing Phishing

Phishing is the most common cyberattack method. Fraudulent emails, texts, or websites impersonate legitimate organizations to trick recipients into revealing passwords, clicking malicious links, or transferring money. It is a numbers game—attackers send millions of messages knowing even a small success rate yields results.

The Anatomy of a Phishing Email

Suspicious sender addresses

The actual email address—not the display name—reveals the true sender. Warning signs: domain mismatches, misspelled domains ("micros0ft.com"), similar-but-wrong domains, suspicious subdomains. Always hover to reveal the full address before trusting a display name.

Suspicious links and URLs

Mismatched link text and destination, misspelled domains, IP addresses instead of domain names, suspicious subdomains, and URL shorteners hiding destinations. Hover to preview before clicking; never trust link text alone.

Artificial urgency and pressure

"Your account will be closed in 24 hours," "Suspicious activity—immediate action required." Urgency short-circuits judgment. Recognize that legitimate organizations rarely create artificial urgency; take time to verify through separate channels.

Dangerous attachments

Office documents with malicious macros, PDFs with embedded exploits, ZIP archives containing malware, and executables disguised with double extensions. Only open attachments from expected, trusted sources; verify unexpected ones through a separate channel.

Fake login pages

Mismatched URLs, missing HTTPS, poor quality design, or unexpected login requests. Never click login links in emails—navigate directly by typing the URL. Password managers help because they won't auto-fill on fake sites with mismatched domains.

Real-World Phishing Examples

A fake Microsoft alert from "microsoft-account-verify.com" with a generic greeting and 24-hour deadline; a fake invoice from an unfamiliar company with a suspicious Word document attachment; a CEO fraud attempt from a ".co" domain requesting an urgent, confidential favor. Each example shares the same red flags: mismatched domains, generic greetings, urgency, and requests to bypass normal verification.

What to Do When You Receive a Phishing Email

Do not click links or open attachments, do not reply, report it to IT or your security contact, and delete it after reporting. If you clicked a link or entered credentials, immediately change the password, change it on any other accounts using the same password, enable MFA, report the incident, and monitor the account.

Building Phishing Recognition Skills

Stay informed about current trends, participate in training and simulated exercises, develop healthy skepticism about unexpected emails, take time to verify rather than act immediately, and report suspicious emails to help protect others. It is always better to verify a legitimate email than fall for a phishing attempt.

Social Engineering

Social engineering encompasses manipulation techniques that exploit human psychology to gain unauthorized access to information, systems, or facilities—targeting people rather than technology.

Why Social Engineering Works

It exploits authority (compliance with perceived authority figures), trust (helpfulness and rapport), urgency (impairing judgment), fear (threats of negative consequences), reciprocity (feeling obligated to return favors), social proof, and scarcity. Effective attacks combine multiple principles to overcome normal skepticism.

Common Social Engineering Techniques

Phone-based social engineering (vishing)

Tech support scams requesting remote access, bank fraud calls requesting account verification, CRA/tax scams threatening arrest, executive impersonation requesting urgent actions, and vendor impersonation. Never provide sensitive information to unsolicited callers; verify by hanging up and calling a known legitimate number.

Tailgating and physical social engineering

Following an authorized person into a restricted area by exploiting politeness. Never hold secure doors for unknown individuals; require everyone to use their own access credentials; report unknown individuals in restricted areas.

Impersonation attacks

IT support impersonation requesting passwords, executive impersonation pressuring subordinates, vendor impersonation, and authority impersonation. Verify identity through independent channels before providing information or access—legitimate IT staff never request passwords.

Fake technical support

Pop-up warnings claiming infection with a support phone number, unsolicited support calls, and fake support websites. Never call numbers from pop-ups or grant remote access to unsolicited callers.

Organizational Defenses Against Social Engineering

- Establish verification procedures using independent communication channels
- Create a security-aware culture where questioning requests is expected, not discouraged
- Implement separation of duties for sensitive actions
- Provide regular training with realistic scenarios
- Document clear policies for sensitive information, access, and payments
- Encourage blame-free reporting
- Test awareness through periodic social engineering tests
- Limit publicly available information useful for reconnaissance

Responding to Social Engineering Attempts

If you suspect an attempt: don't provide information, politely end the interaction, verify through independent channels, report the attempt, and document details. If you realize you've been manipulated: immediately report it, change compromised passwords, revoke granted access, monitor for suspicious activity, and cooperate with response procedures. Falling for a sophisticated attack does not indicate carelessness—it indicates a skilled attacker. Report promptly so appropriate action can be taken.

PART FIVE

Devices and Networks

Browsing, mobile devices, updates, malware, ransomware, and Wi-Fi

Safe Internet Browsing

Web browsers are the primary interface to the internet for most organizational activities, making them essential tools and significant security risks. Modern attacks exploit browser vulnerabilities, use social engineering, create convincing fake websites, and leverage advertising networks to distribute malicious content.

Understanding Browser Security Risks

Malicious websites deliver malware or steal credentials; drive-by downloads install malware automatically; malicious advertisements (malvertising) can appear even on legitimate sites; fake websites impersonate legitimate organizations; browser exploits target vulnerabilities; tracking threats monitor behavior.

Safe Download Practices

- Download only from trusted, official sources
- Verify you're on the legitimate website by checking the URL carefully
- Don't download from unexpected emails or unsolicited links
- Check file types – an invoice should be a PDF, not an executable
- Scan downloads with antivirus software before opening
- Avoid pirated software, which frequently contains malware

Managing Pop-ups and Intrusive Content

Fake security warnings, fake system messages, fake prizes, and fake surveys are common malicious pop-up types. Enable pop-up blocking, never call phone numbers from pop-ups, never download software prompted by pop-ups, and close suspicious pop-ups via the X button rather than clicking any buttons inside them.

HTTPS and Secure Connections

Look for "https://" and a padlock icon before entering sensitive information. HTTPS encrypts communication but does not verify legitimacy—a phishing site can also use HTTPS, so always verify the domain name matches the legitimate organization.

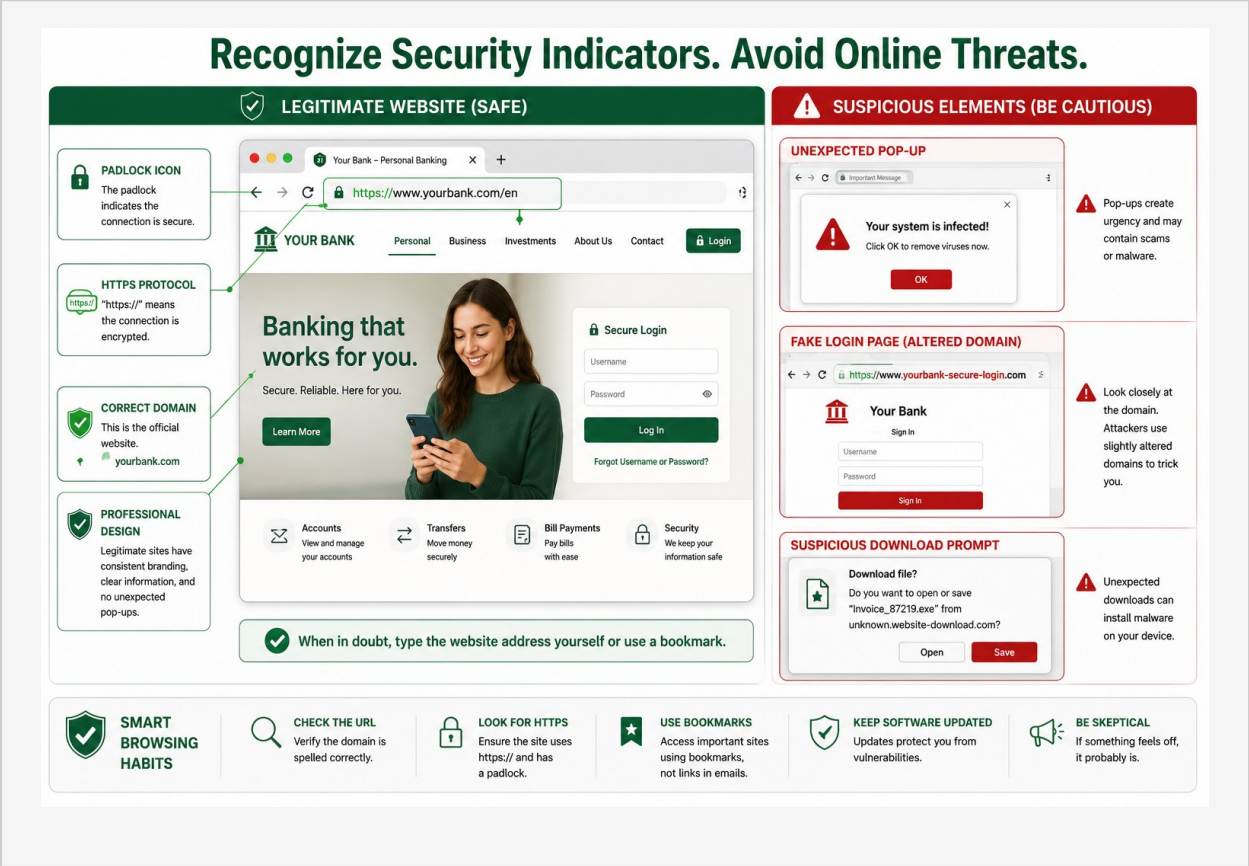
Identifying and Avoiding Fake Websites

Warning signs: domain name variations, poor design quality, unusual requests for sensitive information, suspicious URLs, and missing security indicators. Navigate directly by typing URLs or using bookmarks rather than clicking email links; use password managers that only auto-fill on recognized legitimate domains; enable MFA.

Keeping Your Browser Updated

Enable automatic updates, update all extensions and add-ons, remove unused extensions, and use a modern, actively maintained browser. Combined with email security and phishing recognition skills, safe browsing practices significantly reduce your risk of compromise through web-based

attacks.


Recognize Security Indicators. Avoid Online Threats.
LEGITIMATE WEBSITE (SAFE)
PADLOCK ICON
The padlock indicates the connection is secure.
HTTPS PROTOCOL
"https://" means the connection is encrypted.
CORRECT DOMAIN
This is the official website.
yourbank.com
PROFESSIONAL DESIGN
Legitimate sites have consistent branding, clear information, and no unexpected pop-ups.
Your Bank – Personal Banking
https://www.yourbank.com/en
YOUR BANK
Personal
Business
Investments
About Us
Contact
Login
Banking that works for you.
Secure. Reliable. Here for you.
Learn More
Secure Login
Username
Password
Log In
Forgot Username or Password?
Accounts
View and manage your accounts
Transfers
Move money securely
Bill Payments
Pay bills with ease
Security
We keep your information safe
When in doubt, type the website address yourself or use a bookmark.
SUSPICIOUS ELEMENTS (BE CAUTIOUS)
UNEXPECTED POP-UP
Your system is infected!
Click OK to remove viruses now.
OK
Pop-ups create urgency and may contain scams or malware.
FAKE LOGIN PAGE (ALTERED DOMAIN)
https://www.yourbank-secure-login.com
Your Bank
Sign In
Username
Password
Sign In
Look closely at the domain. Attackers use slightly altered domains to trick you.
SUSPICIOUS DOWNLOAD PROMPT
Download file?
Do you want to open or save "invoice_87219.exe" from unknown.website-download.com?
Open
Save
Unexpected downloads can install malware on your device.
SMART BROWSING HABITS
CHECK THE URL
Verify the domain is spelled correctly.
LOOK FOR HTTPS
Ensure the site uses https:// and has a padlock.
USE BOOKMARKS
Access important sites using bookmarks, not links in emails.
KEEP SOFTWARE UPDATED
Updates protect you from vulnerabilities.
BE SKEPTICAL
If something feels off, it probably is.

Protecting Mobile Devices

Mobile devices—smartphones, tablets, laptops—have become essential business tools, yet present unique challenges: they travel with employees, connect to untrusted networks, and face physical security risks stationary equipment doesn't.

Device Encryption

Encryption makes data unreadable without the correct key. iOS enables encryption by default with a passcode; Android offers encryption, often on by default; Windows uses BitLocker; macOS uses FileVault; Linux uses LUKS. Enable encryption on all devices storing organizational information, use strong passwords, and keep recovery keys secure and separate from the device.

Screen Locks and Authentication

Configure automatic lock after 2-5 minutes of inactivity, use strong PINs (6+ digits) or biometrics, lock immediately on sleep, and disable "Smart Lock" features that keep devices unlocked near trusted locations or devices. Biometric authentication should supplement, not replace, strong passwords for device encryption.

Remote Wipe Capabilities

"Find My iPhone," "Find My Device" (Android), and "Find My Mac" provide remote wipe. Organizations with multiple devices should consider mobile device management (MDM) for centralized control. Enable and test remote wipe before devices are lost; report lost devices immediately.

Mobile Device Security Policies

Define acceptable use, required security controls (encryption, screen locks, updates), lost/stolen device reporting, personal vs. organizational device (BYOD) rules, international travel measures, and device retirement/wiping procedures.

Application Security on Mobile Devices

Install only from official app stores, review permissions before installing, keep applications updated, remove unused applications, and avoid jailbreaking or rooting devices, which disables built-in security protections.


Secure Your Mobile Devices. Protect Your Data Everywhere.
ENCRYPTION
All data is encrypted on the device and in transit.
CLOUD MANAGEMENT
Secure. Monitor. Protect.
REMOTE WIPE
Lost or stolen? Remotely wipe your device and protect your data.
REMOTE WIPE
How it works:
1. Report lost or stolen
2. Send secure wipe command
3. Device receives command
4. Data is erased and device is locked
STRONG DEVICE LOCK
Use a strong passcode or biometric authentication.
10:30
Monday, May 20
Touch ID Authenticated
Device is secure
All systems protected
Device is secure
All systems protected
AUTOMATIC LOCK
Devices lock automatically after a short period of inactivity.
10:30
UNSECURED DEVICE
Missing security controls put your data at risk.
No screen lock
No encryption
Outdated OS
No remote wipe
SECURE DEVICES. PROTECTED DATA. PEACE OF MIND.
Use built-in security features and follow your organization's policies.
THE RISK
Unsecured devices can lead to:
Data breaches
Identity theft
Financial loss
Reputational damage
SECURITY POLICIES IN ACTION
PASSWORD POLICY
Use strong passcodes and change regularly.
BIOMETRIC AUTHENTICATION
Enable fingerprint or face recognition.
SOFTWARE UPDATES
Keep OS and apps up to date.
BACKUP DATA
Back up important data regularly.
REPORT INCIDENTS
Report lost, stolen or suspicious activity immediately.
LEGEND
Secured
At Risk

Software Updates

Software updates address security vulnerabilities, fix bugs, and improve functionality. The failure to apply updates is a leading cause of successful cyberattacks—attackers actively exploit known vulnerabilities in outdated software.

Understanding Update Types

Security updates address specific exploitable vulnerabilities and are highest priority; critical security updates should be applied immediately. Feature updates add functionality and often include security improvements. Cumulative updates include all previous fixes, simplifying management.

The Risks of Unsupported Software

When software reaches end-of-life, vendors stop releasing patches, even for critical vulnerabilities—creating permanent exposure, compliance violations, incompatibility, and unavailable support. Examples: Windows 7, Internet Explorer 11, older Office versions, and legacy server operating systems.

Address unsupported software by inventorying all software, planning migrations before end-of-support, budgeting for upgrades, isolating unavoidable legacy systems, and considering open-source alternatives with longer support lifecycles.

Patch Management

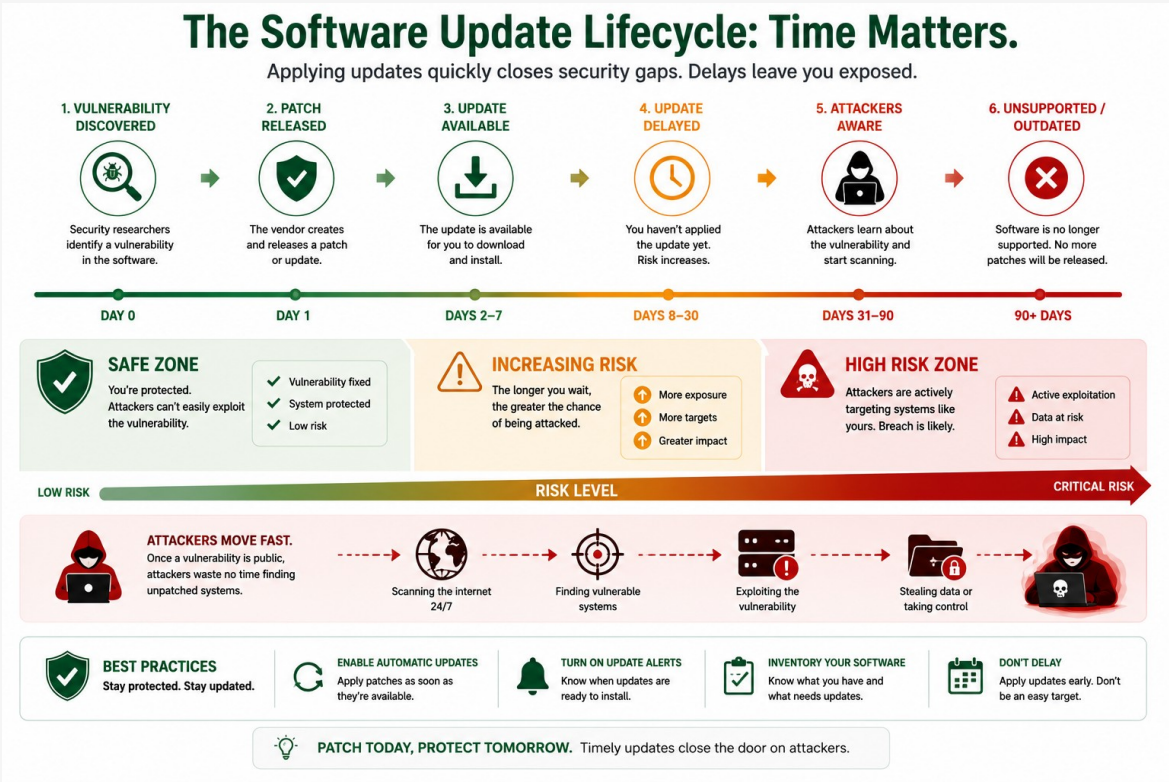
An effective process includes: inventory and monitoring of software and vendor advisories; assessment and prioritization of severity and exploitation risk; testing in non-production environments; systematic deployment starting with critical systems; and verification that patches applied successfully.

Enable automatic updates for personal devices and non-critical systems; use managed automatic updates with testing for business systems; manually manage critical production systems with thorough testing—but never disable updates entirely.

Update Best Practices for Small Organizations

- Enable automatic updates where possible (OS, browsers, mobile devices, security software)
- Establish a monthly update routine, applying security patches available for at least a week
- Prioritize internet-facing systems, systems with sensitive information, and authentication systems
- Back up before major updates and test on one system before wide deployment
- Identify software approaching end-of-support at least six months in advance

The security risk of running outdated, vulnerable software far exceeds the inconvenience of planned maintenance.


The Software Update Lifecycle: Time Matters.
Applying updates quickly closes security gaps. Delays leave you exposed.
1. VULNERABILITY DISCOVERED
Security researchers identify a vulnerability in the software.
2. PATCH RELEASED
The vendor creates and releases a patch or update.
3. UPDATE AVAILABLE
The update is available for you to download and install.
4. UPDATE DELAYED
You haven't applied the update yet. Risk increases.
5. ATTACKERS AWARE
Attackers learn about the vulnerability and start scanning.
6. UNSUPPORTED / OUTDATED
Software is no longer supported. No more patches will be released.
DAY 0
DAY 1
DAYS 2–7
DAYS 8–30
DAYS 31–90
90+ DAYS
SAFE ZONE
You're protected. Attackers can't easily exploit the vulnerability.
Vulnerability fixed
System protected
Low risk
INCREASING RISK
The longer you wait, the greater the chance of being attacked.
More exposure
More targets
Greater impact
HIGH RISK ZONE
Attackers are actively targeting systems like yours. Breach is likely.
Active exploitation
Data at risk
High impact
LOW RISK
RISK LEVEL
CRITICAL RISK
ATTACKERS MOVE FAST.
Once a vulnerability is public, attackers waste no time finding unpatched systems.
Scanning the internet 24/7
Finding vulnerable systems
Exploiting the vulnerability
Stealing data or taking control
BEST PRACTICES
Stay protected. Stay updated.
ENABLE AUTOMATIC UPDATES
Apply patches as soon as they're available.
TURN ON UPDATE ALERTS
Know when updates are ready to install.
INVENTORY YOUR SOFTWARE
Know what you have and what needs updates.
DON'T DELAY
Apply updates early. Don't be an easy target.
PATCH TODAY, PROTECT TOMORROW. Timely updates close the door on attackers.

Malware

Malware (malicious software) is intentionally designed to cause damage, steal information, or gain unauthorized access. Modern malware is developed by sophisticated criminal organizations with clear financial objectives.

Malware Categories

Viruses

Attach to legitimate files and spread when shared or executed, requiring user action. Types include file infectors, macro viruses, and boot sector viruses.

Worms

Self-replicating malware that spreads automatically across networks by exploiting vulnerabilities, without requiring user action—WannaCry (2017) and Conficker (2008) caused widespread damage. Prevention: apply updates promptly, use network segmentation, disable unnecessary services.

Trojans

Disguised as legitimate software, relying on social engineering rather than self-replication. Types include Remote Access Trojans, banking Trojans, downloader Trojans, and fake antivirus Trojans, often distributed via untrusted downloads, pirated software, or malicious ads.

Spyware

Secretly monitors activity and collects information: browsing history, screenshots, files, application usage, and even webcam/microphone access. Often bundled with free software or browser extensions.

Keyloggers

Record every keystroke, capturing passwords before encryption. Software or (less commonly) hardware-based. Multi-factor authentication protects accounts even if passwords are captured.

Malware Infection Methods

Email attachments and malicious links remain primary vectors, along with drive-by downloads, unpatched software vulnerabilities, removable media, pirated software, and supply chain compromise.

Malware Defense Strategies

Prevention:

Keep software updated, use reputable anti-malware, filter email, restrict user permissions, disable Office macros by default, and implement application whitelisting on critical systems.

Detection:

Real-time scanning, behavior monitoring, regular log review, and endpoint detection and response tools where resources permit.

Response:

Isolate infected systems immediately, preserve evidence, remove malware or rebuild from clean backups, change passwords for accessed accounts, and investigate the infection vector to prevent recurrence.

Ransomware

Ransomware encrypts an organization's files and systems, demanding payment for the decryption key. Modern operations often combine encryption with data theft, threatening to publish stolen information ("double extortion") if ransom is not paid.

How Ransomware Works

Initial access via phishing, exploited vulnerabilities, compromised credentials (RDP/VPN), malicious websites, or supply chain compromise. Sophisticated operators then conduct reconnaissance and lateral movement—mapping networks, escalating privileges, disabling security tools, and stealing data—before deploying encryption and a ransom demand, often in cryptocurrency with a deadline.

Common Ransomware Entry Points

Phishing emails, exposed Remote Desktop Protocol (RDP), unpatched internet-facing systems, malicious advertisements, and compromised software updates.

Recovery from Ransomware

Option 1: Restore from backups (preferred)

Requires recent, complete, offline or immutable backups and tested restoration procedures.

Option 2: Attempt decryption without paying

Check resources like No More Ransom (nomoreransom.org) for available decryption tools for specific variants.

Option 3: Pay the ransom (not recommended)

No guarantee of decryption, funds criminal operations, may violate sanctions law, and organizations that pay are often targeted again. Never rely on payment as a recovery strategy—invest instead in prevention and resilience.

Ransomware Prevention

Technical controls:

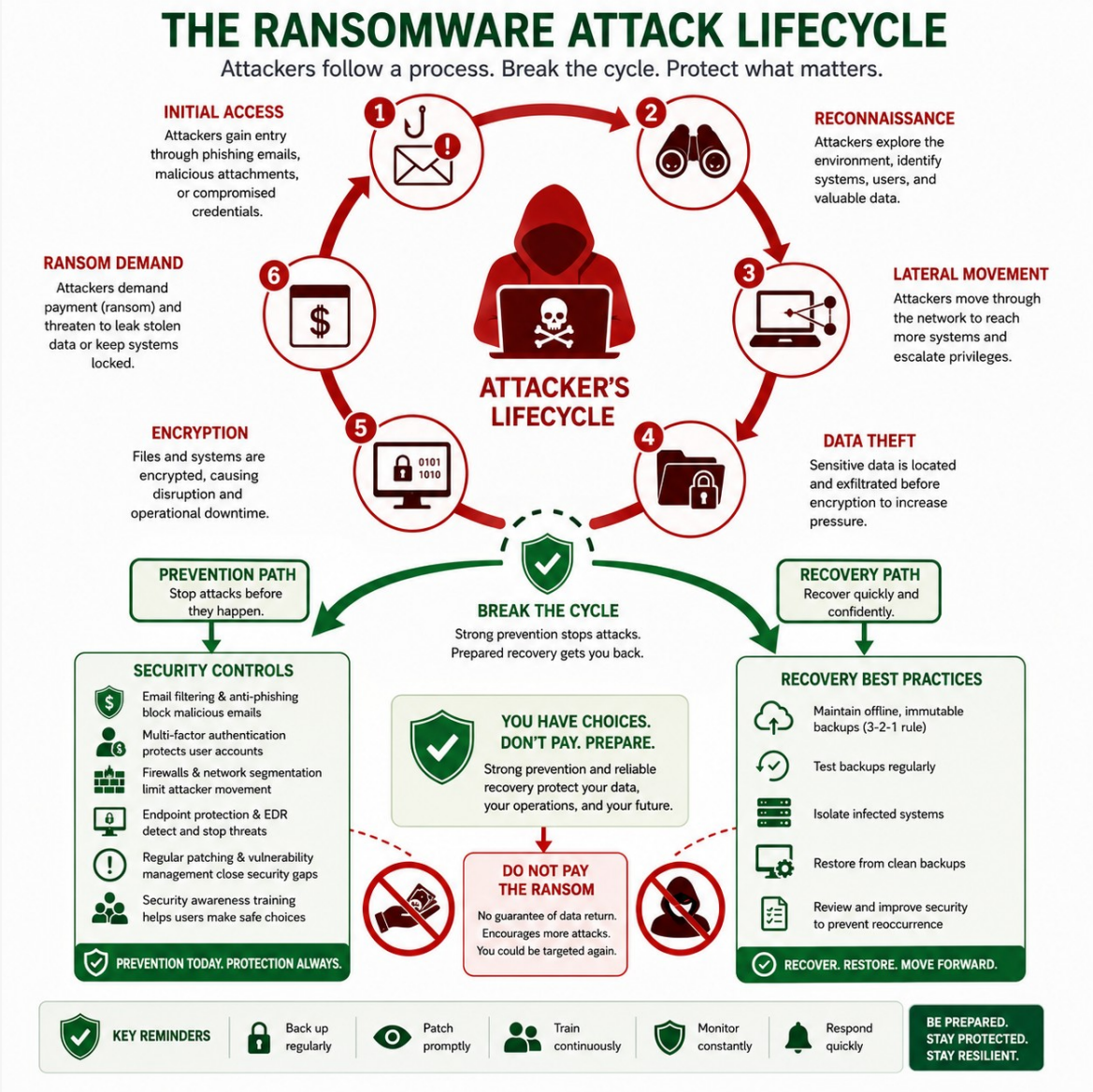
Updated systems, email filtering, disabled macros by default, restricted admin privileges, application whitelisting, EDR tools, network segmentation, secured or disabled RDP, and MFA for remote access.

Backup strategies:

Regular automated backups following the 3-2-1 rule, offline or immutable storage, and regularly tested restoration.

User awareness and incident response planning:

Phishing training, simulated exercises, ransomware-specific response procedures, and tabletop exercises. The ability to recover without paying depends entirely on preparation made before an attack occurs.


THE RANSOMWARE ATTACK LIFECYCLE
Attackers follow a process. Break the cycle. Protect what matters.
1
INITIAL ACCESS
Attackers gain entry through phishing emails, malicious attachments, or compromised credentials.
2
RECONNAISSANCE
Attackers explore the environment, identify systems, users, and valuable data.
3
LATERAL MOVEMENT
Attackers move through the network to reach more systems and escalate privileges.
4
DATA THEFT
Sensitive data is located and exfiltrated before encryption to increase pressure.
5
ENCRYPTION
Files and systems are encrypted, causing disruption and operational downtime.
6
RANSOM DEMAND
Attackers demand payment (ransom) and threaten to leak stolen data or keep systems locked.
ATTACKER'S LIFECYCLE
BREAK THE CYCLE
Strong prevention stops attacks.
Prepared recovery gets you back.
PREVENTION PATH
Stop attacks before they happen.
SECURITY CONTROLS
Email filtering & anti-phishing block malicious emails
Multi-factor authentication protects user accounts
Firewalls & network segmentation limit attacker movement
Endpoint protection & EDR detect and stop threats
Regular patching & vulnerability management close security gaps
Security awareness training helps users make safe choices
PREVENTION TODAY. PROTECTION ALWAYS.
YOU HAVE CHOICES. DON'T PAY. PREPARE.
Strong prevention and reliable recovery protect your data, your operations, and your future.
DO NOT PAY THE RANSOM
No guarantee of data return.
Encourages more attacks.
You could be targeted again.
RECOVERY PATH
Recover quickly and confidently.
RECOVERY BEST PRACTICES
Maintain offline, immutable backups (3-2-1 rule)
Test backups regularly
Isolate infected systems
Restore from clean backups
Review and improve security to prevent reoccurrence
RECOVER. RESTORE. MOVE FORWARD.
KEY REMINDERS
Back up regularly
Patch promptly
Train continuously
Monitor constantly
Respond quickly
BE PREPARED.
STAY PROTECTED.
STAY RESILIENT.

Secure Wi-Fi

Wireless networks provide essential connectivity but introduce risks that wired networks do not face, since signals extend beyond physical boundaries.

Home Wi-Fi Security

- Change default router administrator credentials
- Use WPA3 or WPA2 encryption; never WEP or open networks
- Set a strong, unique Wi-Fi password (12+ characters)
- Disable WPS and remote management
- Update router firmware regularly
- Review connected devices periodically

Office Wi-Fi Security

Use enterprise authentication (WPA2/WPA3-Enterprise with individual RADIUS logins rather than a shared password), strong encryption, network segmentation via VLANs, wireless intrusion detection, physical security of access points, and regular assessments. MAC address filtering provides minimal security and should not be relied upon.

Guest Wi-Fi Networks

Guest networks must be completely isolated from internal systems, use a captive portal with acceptable use terms, limit bandwidth, consider time-limited access, apply content filtering, and be monitored for abuse.

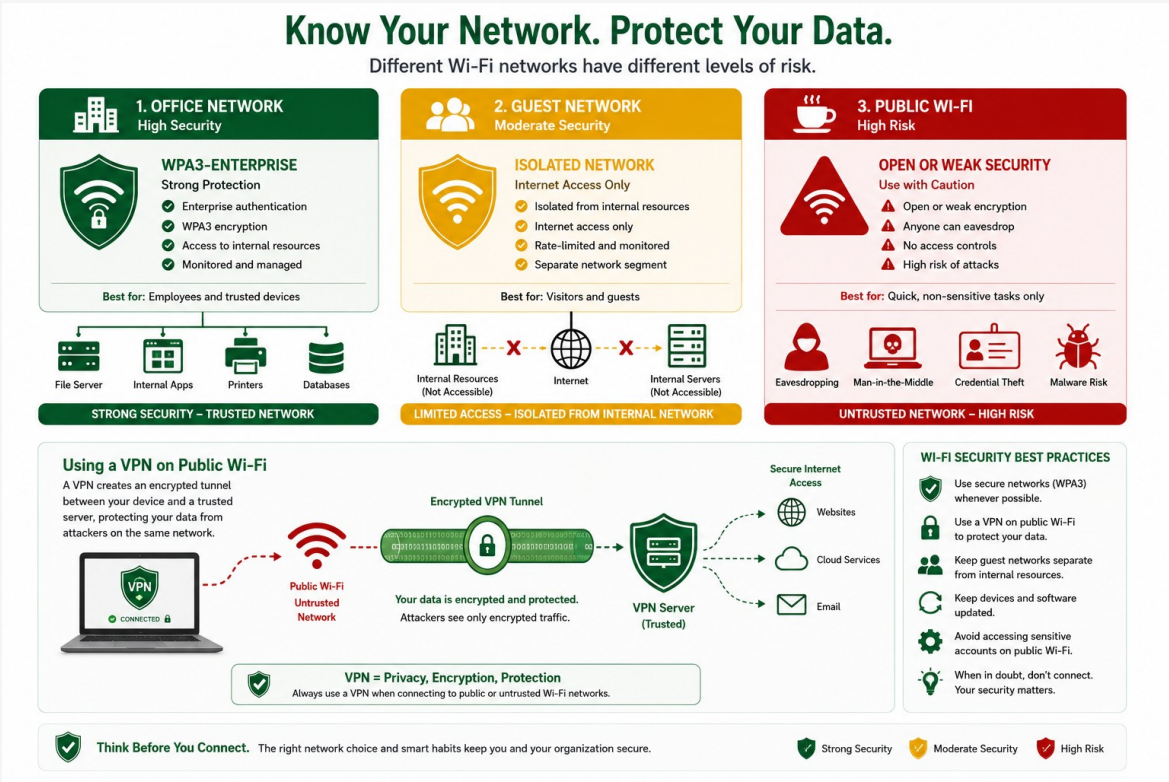
Public Wi-Fi Risks

Unencrypted communications, man-in-the-middle attacks, rogue access points mimicking legitimate names, malware distribution, and session hijacking are common threats. Avoid sensitive activities, verify network names with staff, disable automatic connection, use HTTPS, disable file sharing, and always use a VPN.

Virtual Private Networks (VPNs)

A VPN creates an encrypted tunnel between your device and a VPN server, protecting all traffic from interception, essential for public Wi-Fi and remote access. Organizations should provide VPN access for remote/traveling employees; for personal use, choose reputable providers with no-logs policies and avoid free VPN services that may monetize data.

Wireless security requires different approaches for home, office, guest, and public networks, with VPN use essential wherever networks cannot be trusted.


Know Your Network. Protect Your Data.
Different Wi-Fi networks have different levels of risk.
1. OFFICE NETWORK
High Security
WPA3-ENTERPRISE
Strong Protection
Enterprise authentication
WPA3 encryption
Access to internal resources
Monitored and managed
Best for: Employees and trusted devices
File Server
Internal Apps
Printers
Databases
STRONG SECURITY – TRUSTED NETWORK
2. GUEST NETWORK
Moderate Security
ISOLATED NETWORK
Internet Access Only
Isolated from internal resources
Internet access only
Rate-limited and monitored
Separate network segment
Best for: Visitors and guests
Internal Resources (Not Accessible)
Internet
Internal Servers (Not Accessible)
LIMITED ACCESS – ISOLATED FROM INTERNAL NETWORK
3. PUBLIC WI-FI
High Risk
OPEN OR WEAK SECURITY
Use with Caution
Open or weak encryption
Anyone can eavesdrop
No access controls
High risk of attacks
Best for: Quick, non-sensitive tasks only
Eavesdropping
Man-in-the-Middle
Credential Theft
Malware Risk
UNTRUSTED NETWORK – HIGH RISK
Using a VPN on Public Wi-Fi
A VPN creates an encrypted tunnel between your device and a trusted server, protecting your data from attackers on the same network.
VPN
CONNECTED
Public Wi-Fi
Untrusted
Network
Encrypted VPN Tunnel
Your data is encrypted and protected.
Attackers see only encrypted traffic.
VPN Server
(Trusted)
Secure Internet Access
Websites
Cloud Services
Email
VPN = Privacy, Encryption, Protection
Always use a VPN when connecting to public or untrusted Wi-Fi networks.
WI-FI SECURITY BEST PRACTICES
Use secure networks (WPA3) whenever possible.
Use a VPN on public Wi-Fi to protect your data.
Keep guest networks separate from internal resources.
Keep devices and software updated.
Avoid accessing sensitive accounts on public Wi-Fi.
When in doubt, don't connect. Your security matters.
Think Before You Connect. The right network choice and smart habits keep you and your organization secure.
Strong Security
Moderate Security
High Risk

PART SIX

Work Environments

Remote work, cloud services, and backups

Remote Work Security

Remote work provides flexibility but introduces security challenges absent from traditional offices, as employees access systems from diverse locations, networks, and devices outside direct organizational control.

Working from Home

Secure home Wi-Fi, establish a dedicated workspace with lockable storage, use VPN for internal resources, enable firewalls, keep software updated, separate work and personal activities where possible, use secure video conferencing and be mindful of visible backgrounds, ensure family members understand device confidentiality, and consider backup internet connectivity for critical work.

Coffee Shops and Public Spaces

Always use VPN; never leave devices unattended; use privacy screens and position yourself so your screen isn't visible; avoid sensitive activities where you can't control observation; verify legitimate Wi-Fi network names with staff; disable automatic connections; use headphones for confidential calls; and be cautious of helpful strangers.

Travel Security

Before traveling: back up devices, update software, remove unnecessary sensitive information, and confirm VPN works at your destination. While traveling: keep devices with you at all times, use VPN on hotel Wi-Fi, disable Bluetooth/Wi-Fi when not needed, and avoid public USB charging stations.

At border crossings, understand that agents in many countries can search devices and that biometric authentication can be compelled in ways passwords cannot; some organizations provide "clean" devices for international travel. After travel: scan for malware, change passwords used during travel, and report any suspicious device tampering.

Shared Computers

Avoid using shared computers for organizational work whenever possible. If unavoidable: minimize sensitive activities, use private browsing, never save passwords, log out completely, clear browsing data, and assume monitoring may be present. Change any passwords used on a shared computer as soon as you have access to a trusted device.

Remote Work Security Policies

Organizations should define approved and prohibited locations, required security controls, acceptable personal device use, lost/stolen device reporting, travel procedures, and restrictions on shared computers—while providing necessary tools, training, and ongoing support.


Remote Work Anywhere. Security Matters Everywhere.
Your environment and choices affect your security. Make smart decisions.
1. SECURE HOME OFFICE
High Security
Privacy Screen
Secure Wi-Fi (Home Network)
Private, quiet workspace
Locked door / physical security
Secure Wi-Fi (WPA3)
VPN connected
Privacy screen enabled
Company device with updates
Strong password / MFA
BEST CHOICE
Your data stays private and protected.
2. COFFEE SHOP
Moderate Security
Privacy Screen
Public Wi-Fi
Use VPN
Privacy screen enabled
Avoid handling sensitive info
Log out of sessions
Be aware of your surroundings
Avoid file sharing / printers
OK WITH CAUTION
Stay alert and minimize risks.
3. AIRPORT / TRAVEL
Moderate Security
Public Wi-Fi (Untrusted)
Use VPN at all times
Do not access sensitive data
Verify websites (https://)
Keep devices close
Disable file sharing / Airdrop
Watch for shoulder surfing
HIGHER RISK
Necessary, but be extra careful.
4. SHARED COMPUTER
High Risk
Sessions may be monitored
Keyloggers may be installed
Data may be saved or stolen
Do NOT use for sensitive work
Avoid saving passwords
Do not access company systems
Log out completely
Clear browser history
Use your own device instead
AVOID WHEN POSSIBLE
High risk of data exposure and theft.
REMOTE WORK SECURITY BEST PRACTICES
Use VPN
Encrypt your connection.
Keep Devices Updated
Install updates regularly.
Enable MFA
Add extra protection to your accounts.
Use Secure Networks
Avoid open or untrusted Wi-Fi.
Be Security Aware
Think before you click or download.
Back Up Regularly
Protect your data against loss.
Think. Protect. Connect. Smart choices keep your work—and your data—secure, wherever you are.

Cloud Security Basics

Cloud computing offers scalability, accessibility, and reduced infrastructure costs, but introduces security considerations governed by the shared responsibility model: security is shared between the provider and the customer organization.

The Cloud Responsibility Model

Infrastructure as a Service (IaaS)

Provider secures physical infrastructure and hypervisor; customer is responsible for the operating system, applications, data encryption, access controls, and backups—the most customer responsibility of the three models.

Platform as a Service (PaaS)

Provider manages infrastructure and platform/OS updates; customer remains responsible for application security, data, access controls, and backups.

Software as a Service (SaaS)

Provider manages most of the technology stack; customer remains responsible for user access management, data classification and handling, security configuration, training, and monitoring.

Understanding Your Cloud Security Responsibilities

Regardless of service type, customers always retain responsibility for identity and access management, data protection and classification, security configuration, monitoring and incident response, and regulatory compliance.

Cloud Data Backup

A common misconception is that cloud data is automatically backed up against all loss. Provider redundancy protects against hardware failure but not accidental deletion, malicious deletion, ransomware, or account compromise. Understand your provider's retention policies (e.g., Microsoft 365 retains deleted items 30-93 days), implement third-party backup (Veeam, Datto, Backupify), test restoration, maintain local copies of critical data, and enable file versioning.

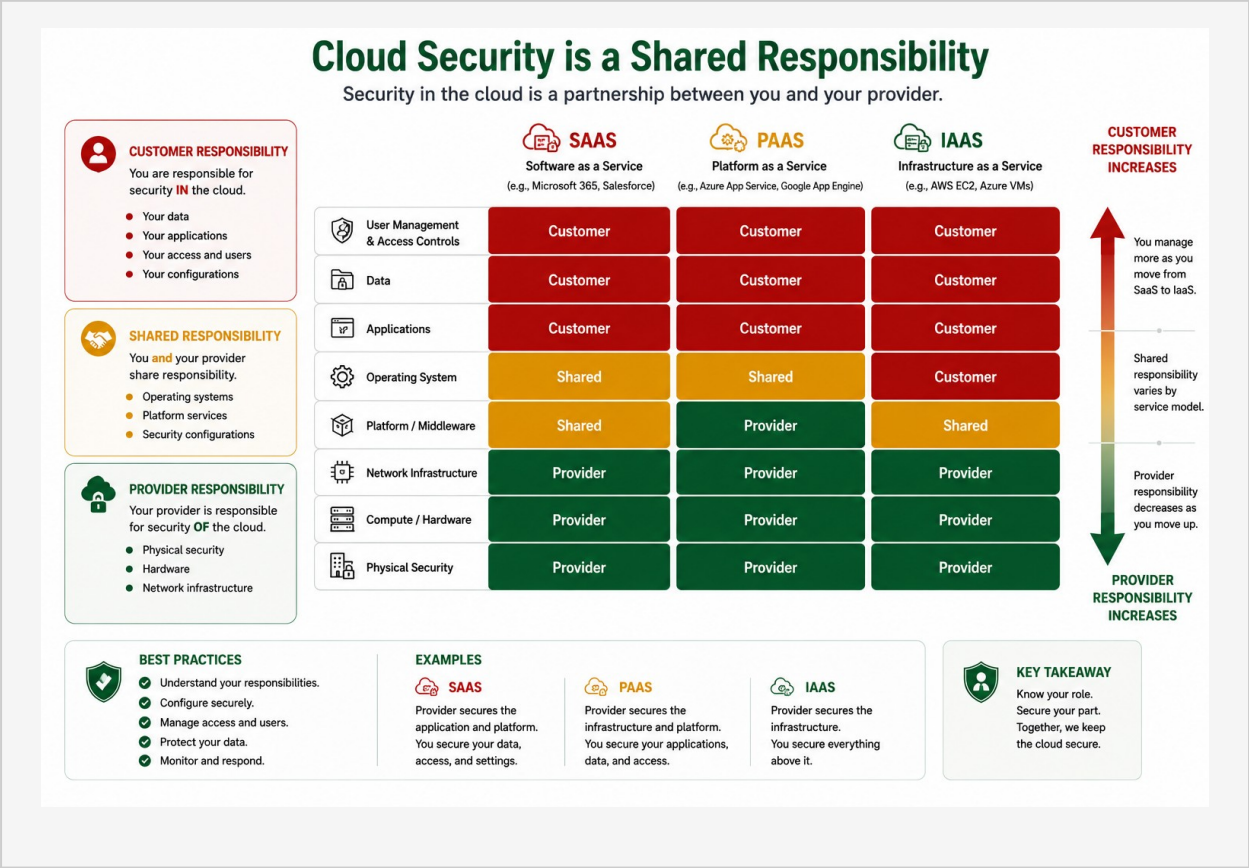
Cloud Permissions and Access Control

Apply the principle of least privilege, conduct regular access reviews, manage shared links carefully (public vs. organization-only vs. specific-user vs. expiring vs. password-protected), establish external sharing policies, manage service accounts and API keys, and require MFA for all cloud accounts.

Cloud Storage and Application Security

Understand encryption in transit, at rest, and client-side; secure sync clients and configure selective sync; set restrictive default sharing; enable activity monitoring and data loss prevention. Maintain an inventory of cloud applications (including "shadow IT"), assess vendor security (certifications, data location, encryption, incident response), implement single sign-on, and secure API keys.

Cloud services offer significant benefits but require active security management—simply moving to the cloud does not automatically make data more secure.



Backups

Backups are the foundation of organizational resilience. No matter how robust your security controls, incidents will occur, and recovery depends entirely on having recent, complete, tested backups.

The 3-2-1 Backup Rule

3 copies of your data (original plus two backups), 2 different media types (e.g., NAS and cloud), 1 offsite copy (physically separate location). Example: nightly backup to a local NAS, weekly backup to rotated offsite external drives, and continuous or daily backup to cloud storage—covering hardware failure, ransomware, and site disasters respectively.

Backup Frequency and Retention

Frequency determines how much data you can afford to lose; critical systems warrant daily or continuous backups. Common retention: daily backups 30 days, weekly 3 months, monthly 1 year, annual 7 years (or as required by regulation).

Offline and Immutable Backups

Ransomware specifically targets backups, encrypting or deleting them to force payment. Offline backups are physically disconnected (rotated external drives, disconnected after backup); immutable backups cannot be modified or deleted for a specified period. Rotate drives keeping at least one disconnected at all times, use backup software supporting immutability, and store backup credentials separately from system credentials.

What to Back Up

User files and documents, databases, email, configuration files, user profiles, websites, financial records, and legal documents—plus system information such as OS configurations, application installations, network configurations, and security settings.

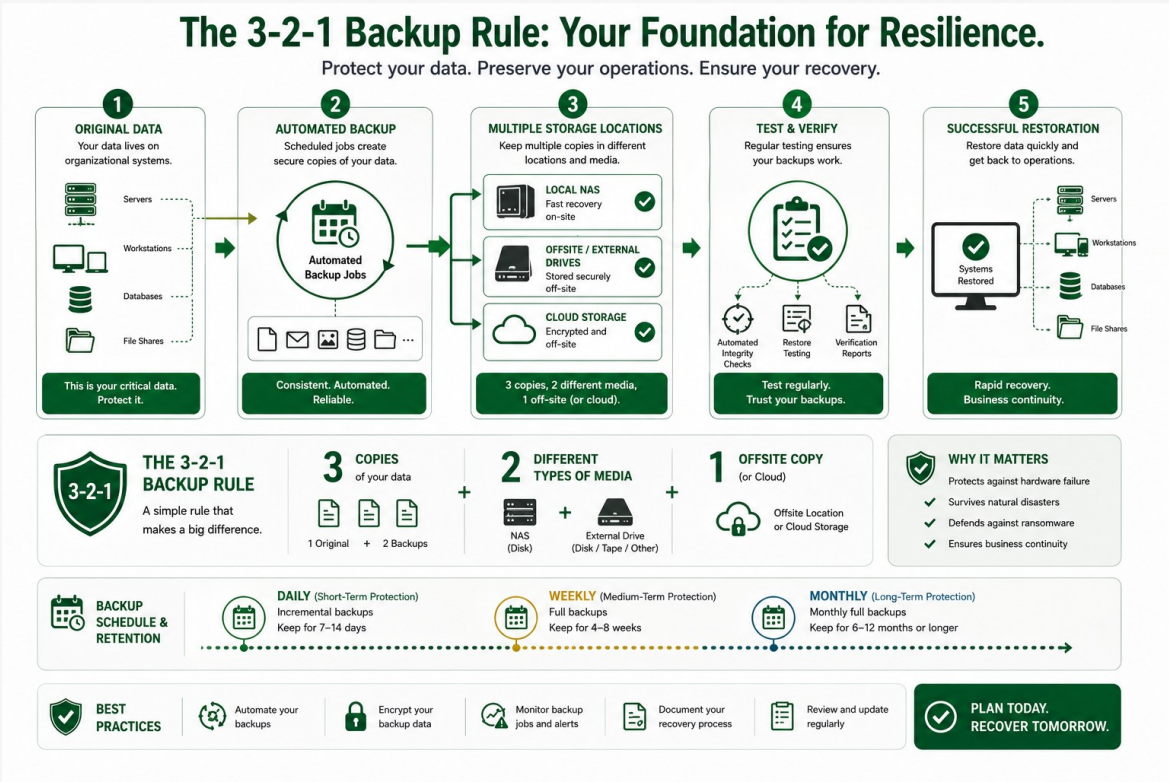
Testing Backup Restoration

Untested backups are not backups—they are hopes. Perform regular restoration tests of files, at least annual full system restoration tests, document procedures clearly, test different scenarios and sources, verify backup integrity, and time restoration to inform recovery expectations.

Backup Monitoring and Maintenance

Review backup logs daily, monitor storage capacity, verify schedules, update configurations as systems change, maintain backup hardware, review retention policies, secure backup credentials with MFA, and document backup infrastructure thoroughly.

Combined with the security practices throughout this guide, robust, tested backups enable organizations to recover from incidents and continue operations even when other defenses fail.


The 3-2-1 Backup Rule: Your Foundation for Resilience.
Protect your data. Preserve your operations. Ensure your recovery.
1
ORIGINAL DATA
Your data lives on organizational systems.
Servers
Workstations
Databases
File Shares
This is your critical data. Protect it.
2
AUTOMATED BACKUP
Scheduled jobs create secure copies of your data.
Automated Backup Jobs
Consistent. Automated. Reliable.
3
MULTIPLE STORAGE LOCATIONS
Keep multiple copies in different locations and media.
LOCAL NAS
Fast recovery on-site
OFFSITE / EXTERNAL DRIVES
Stored securely off-site
CLOUD STORAGE
Encrypted and off-site
3 copies, 2 different media, 1 off-site (or cloud).
4
TEST & VERIFY
Regular testing ensures your backups work.
Automated Integrity Checks
Restore Testing
Verification Reports
Test regularly. Trust your backups.
5
SUCCESSFUL RESTORATION
Restore data quickly and get back to operations.
Systems Restored
Servers
Workstations
Databases
File Shares
Rapid recovery. Business continuity.
3-2-1
THE 3-2-1 BACKUP RULE
A simple rule that makes a big difference.
3 COPIES of your data
1 Original + 2 Backups
2 DIFFERENT TYPES OF MEDIA
NAS (Disk)
External Drive (Disk / Tape / Other)
1 OFFSITE COPY (or Cloud)
Offsite Location or Cloud Storage
WHY IT MATTERS
Protects against hardware failure
Survives natural disasters
Defends against ransomware
Ensures business continuity
BACKUP SCHEDULE & RETENTION
DAILY (Short-Term Protection)
Incremental backups
Keep for 7–14 days
WEEKLY (Medium-Term Protection)
Full backups
Keep for 4–8 weeks
MONTHLY (Long-Term Protection)
Monthly full backups
Keep for 6–12 months or longer
BEST PRACTICES
Automate your backups
Encrypt your backup data
Monitor backup jobs and alerts
Document your recovery process
Review and update regularly
PLAN TODAY. RECOVER TOMORROW.

PART SEVEN

Information and Access Governance

Protecting sensitive data, least privilege, physical security, and vendors

Protecting Sensitive Information

Organizations handle sensitive information throughout its lifecycle—creation, storage, transmission, use, and disposal. Each stage presents risks requiring appropriate safeguards.

Encryption for Data Protection

Encryption at rest

Protects stored data using full disk encryption (BitLocker, FileVault, LUKS), file/folder encryption for defense in depth, database encryption, and cloud storage encryption. Store recovery keys securely, separate from encrypted devices.

Encryption in transit

HTTPS for websites, encrypted email for sensitive communications, VPN for remote access, and secure file transfer protocols (SFTP, HTTPS) rather than insecure ones (FTP, HTTP). Never send highly sensitive information via unencrypted channels.

Need-to-Know Principle

Limit access to sensitive information to only those who require it. Evaluate access requirements before granting, limit scope to specific information needed, conduct regular access reviews, and assign access by role rather than individual. This is about minimizing risk, not distrust.

Secure Sharing Practices

Internal sharing

Use organizational systems rather than personal email, verify recipients before sending, grant only necessary permissions, use expiring links for temporary needs, and avoid public sharing links.

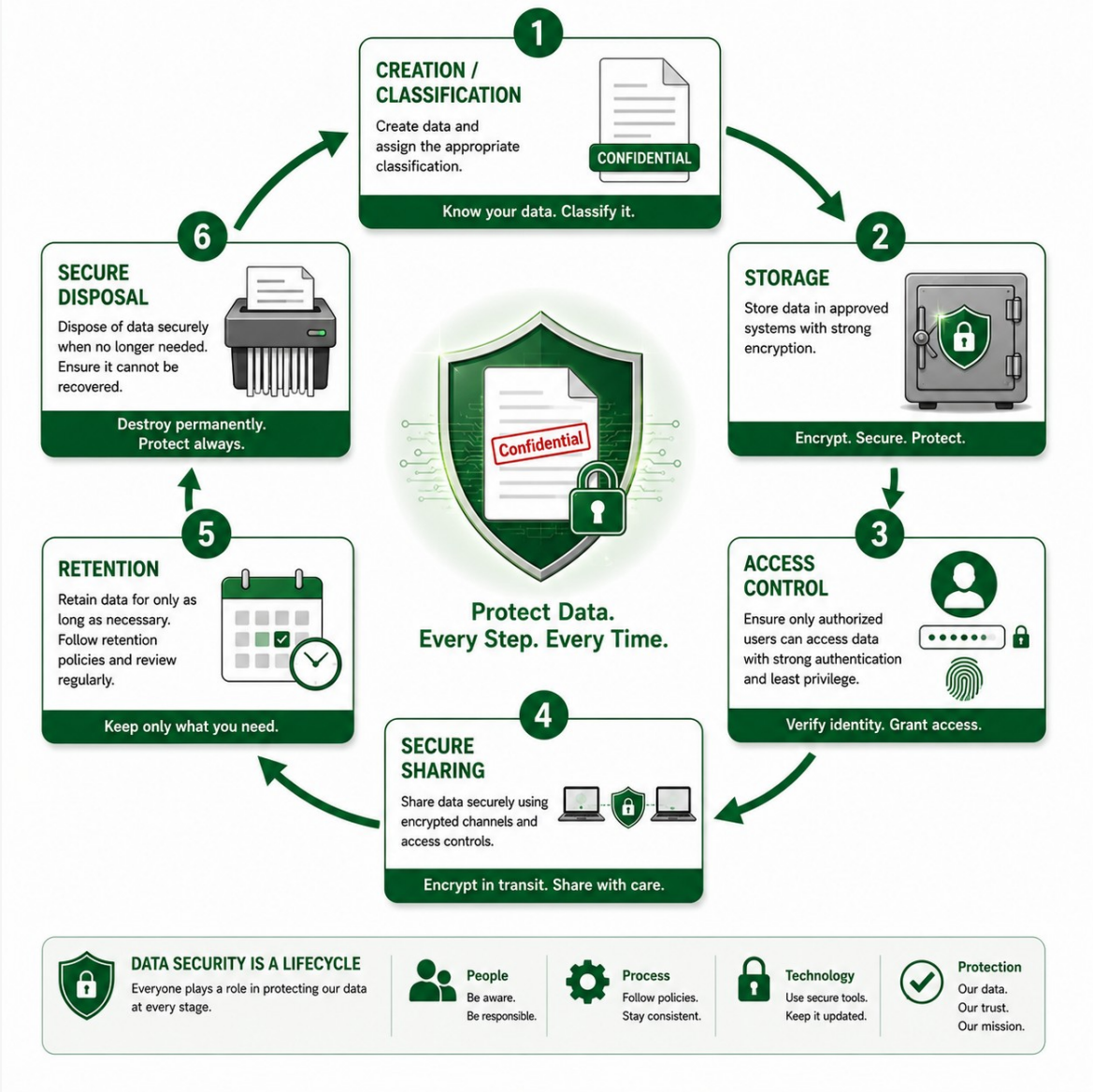
External sharing

Verify recipient identity, use secure/encrypted methods for highly sensitive information, ensure confidentiality agreements are in place, track what was shared externally, and revoke access promptly when no longer needed.

Information Retention and Disposal

Retention policies specify how long information is kept based on legal/regulatory requirements and business needs. Common periods: financial records 7 years, employee records 7 years post-employment, contracts duration plus 7 years.

Secure disposal: use secure deletion tools that overwrite data (simple deletion is insufficient); wipe or destroy storage media before disposal or repurposing; shred sensitive paper documents with a cross-cut shredder; consider secure disposal services with certificates of destruction.


1
CREATION / CLASSIFICATION
Create data and assign the appropriate classification.
CONFIDENTIAL
Know your data. Classify it.
2
STORAGE
Store data in approved systems with strong encryption.
Encrypt. Secure. Protect.
3
ACCESS CONTROL
Ensure only authorized users can access data with strong authentication and least privilege.
Verify identity. Grant access.
4
SECURE SHARING
Share data securely using encrypted channels and access controls.
Encrypt in transit. Share with care.
5
RETENTION
Retain data for only as long as necessary. Follow retention policies and review regularly.
Keep only what you need.
6
SECURE DISPOSAL
Dispose of data securely when no longer needed. Ensure it cannot be recovered.
Destroy permanently. Protect always.
Confidential
Protect Data.
Every Step. Every Time.
DATA SECURITY IS A LIFECYCLE
Everyone plays a role in protecting our data at every stage.
People
Be aware.
Be responsible.
Process
Follow policies.
Stay consistent.
Technology
Use secure tools.
Keep it updated.
Protection
Our data.
Our trust.
Our mission.

User Accounts and Least Privilege

How user accounts are created, managed, and removed significantly impacts security. Least privilege—providing the minimum access necessary—limits the impact of compromised accounts and insider threats.

The Principle of Least Privilege

Limits breach impact, reduces insider threat risk, minimizes mistake consequences, and supports compliance. Implement by defaulting to minimal access, assigning access by role, conducting regular reviews, and granting temporary elevated access only when needed.

The Risks of Administrator Accounts

Administrator accounts are attractive attack targets, amplify malware impact and mistakes, and complicate audit trails when used for routine work.

Best practices:

- Separate standard and administrator accounts for the same person
- Minimize the number of users with administrator access
- Require strong passwords (20+ characters) and MFA without exception
- Monitor and log all administrator account activity
- Disable unnecessary built-in administrator accounts
- Consider time-limited administrative access for specific tasks

Managing User Account Lifecycle

Creation:

Verify authorization, apply least privilege from the start, require strong authentication, and provide training before access is granted.

Ongoing management:

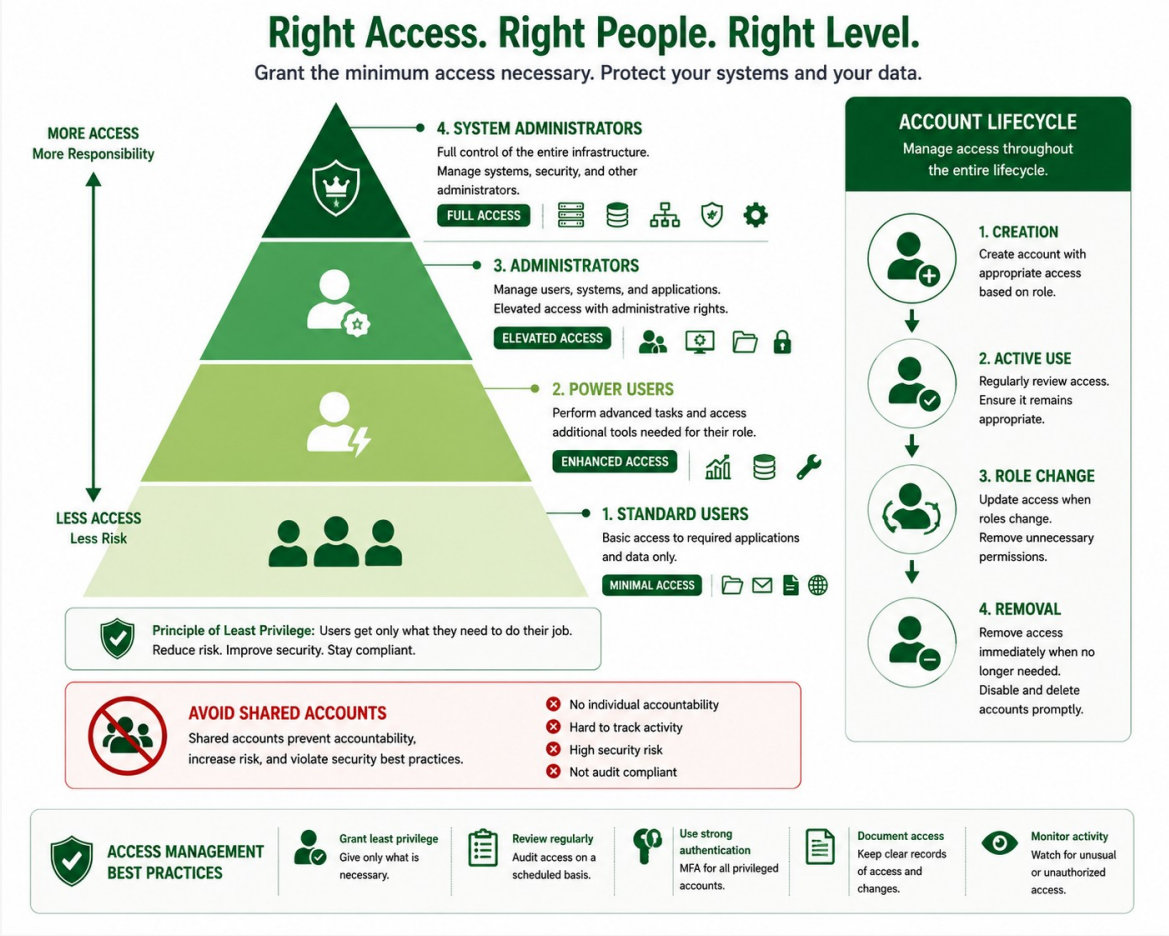
Regular access reviews, prompt updates on role changes, monitoring for suspicious activity, and enforced password policies.

Removal:

Disable accounts immediately upon departure; remove access comprehensively across all systems (email, file sharing, applications, physical access, VPN, vendor portals); transfer ownership of resources first; preserve data for appropriate retention periods; and document removal.

The Dangers of Shared Accounts

Shared accounts create no accountability, credential sharing risks, difficulty revoking access when someone leaves, no effective MFA, and compliance violations. Use individual accounts with appropriate permissions, role-based groups, or monitored service accounts instead. Where shared accounts are unavoidable, log usage, change passwords regularly, and limit permissions as much as possible.


Right Access. Right People. Right Level.
Grant the minimum access necessary. Protect your systems and your data.
MORE ACCESS
More Responsibility
LESS ACCESS
Less Risk
4. SYSTEM ADMINISTRATORS
Full control of the entire infrastructure.
Manage systems, security, and other administrators.
FULL ACCESS
3. ADMINISTRATORS
Manage users, systems, and applications.
Elevated access with administrative rights.
ELEVATED ACCESS
2. POWER USERS
Perform advanced tasks and access additional tools needed for their role.
ENHANCED ACCESS
1. STANDARD USERS
Basic access to required applications and data only.
MINIMAL ACCESS
Principle of Least Privilege: Users get only what they need to do their job. Reduce risk. Improve security. Stay compliant.
AVOID SHARED ACCOUNTS
Shared accounts prevent accountability, increase risk, and violate security best practices.
No individual accountability
Hard to track activity
High security risk
Not audit compliant
ACCOUNT LIFECYCLE
Manage access throughout the entire lifecycle.
1. CREATION
Create account with appropriate access based on role.
2. ACTIVE USE
Regularly review access. Ensure it remains appropriate.
3. ROLE CHANGE
Update access when roles change. Remove unnecessary permissions.
4. REMOVAL
Remove access immediately when no longer needed. Disable and delete accounts promptly.
ACCESS MANAGEMENT BEST PRACTICES
Grant least privilege
Give only what is necessary.
Review regularly
Audit access on a scheduled basis.
Use strong authentication
MFA for all privileged accounts.
Document access
Keep clear records of access and changes.
Monitor activity
Watch for unusual or unauthorized access.

Physical Security

Cybersecurity extends beyond digital protections to physical measures that prevent unauthorized physical access to systems, devices, and information—often the easiest way to bypass digital controls entirely.

Clean Desk Policy

Secure sensitive documents in locked drawers when not in use, clear work surfaces before leaving, lock screens when stepping away, secure portable devices and storage media, and shred sensitive documents rather than discarding them. This prevents shoulder surfing, protects information during after-hours access or cleaning services, and demonstrates security awareness.

Locked Doors and Access Control

Secure building entrances, issue access credentials only to authorized individuals, implement after-hours security, and require visitor sign-in and escorts. Lock individual offices when unoccupied; revoke access promptly on departure; prohibit tailgating; and encourage employees to challenge unknown individuals politely.

Server Room and Equipment Security

Restrict server room access to authorized individuals only, log access, keep doors locked, implement environmental controls (fire suppression, temperature, humidity), and consider surveillance. Lock equipment racks, secure cables, and store backup media in locked, fireproof locations. Consider a two-person rule for sensitive operations and always escort visitors.

Visitor Management

Require sign-in with name, organization, and purpose; issue visible visitor badges collected at departure; escort visitors in secure areas; limit access to only necessary areas; verify vendor and contractor identities; and train reception staff and employees to recognize and report unescorted visitors.

USB Devices and Removable Media

USB drives can introduce malware, enable data theft, or cause data loss. Disable unused USB ports, restrict use to approved devices, scan all devices before use, require encryption on organizational USB drives, and never connect unknown devices found in public areas. Encourage network or cloud file transfer as a safer alternative.


PHYSICAL SECURITY: EVERY LAYER PROTECTS
People. Processes. Protection.
SECURITY LAYERS
1. PERIMETER
Controlled access to the building
2. RECEPTION
Visitors verified and logged
3. WORKSTATIONS
Clean desks. Lock drawers. Protect devices.
4. OFFICES
Keep doors locked when unoccupied
5. SERVER ROOM
Restricted access. Authorized personnel only.
6. SURVEILLANCE
Cameras in key areas
7. EQUIPMENT STORAGE
Lock cabinets and secure assets
LAYERED SECURITY STRONGER TOGETHER
Multiple layers deter threats and reduce risk.
1. LOCKED ENTRANCE
Access control badge required
2. RECEPTION
Visitor sign-in and badge issued
4. LOCKED OFFICE DOORS
Keep doors locked when unoccupied
VIOLATION
Office door left unlocked
5. SECURED SERVER ROOM
Restricted access. Environment monitored. Keep systems secure.
Our Security Is Everyone's Responsibility
VIOLATION
Unattended visitor in restricted area
3. CLEAN DESKS
Lock drawers. No sensitive info left out.
VIOLATION
USB drive left unattended
6. SURVEILLANCE CAMERAS
Monitor entrances, hallways, and critical area.
7. LOCKED EQUIPMENT CABINETS
Store devices and media securely.
COMMON VIOLATIONS
Doors left unlocked
Unattended visitors
Sensitive items left out
Keys or access cards shared
Equipment not secured
BEST PRACTICES
Lock it.
Sign it.
Secure it.
Report it.
Every time.
A SECURE ENVIRONMENT PROTECTS WHAT MATTERS
Lock doors and devices
Verify visitors and contractors
Be aware of your surroundings
Protect keys, cards, and codes
Secure assets and media
Report suspicious activity
SECURITY IS A TEAM EFFORT. THANK YOU FOR DOING YOUR PART.

Working with Vendors

Organizations rely on numerous vendors for technology, software, and business operations. These relationships provide value but introduce security risks—vendor failures can directly impact your organization.

Understanding Third-Party Risk

Data breaches at vendors with access to your data, service disruptions affecting dependent operations, supply chain attacks reaching you through vendors, compliance violations, and reputational damage even when the failure wasn't directly yours.

Questions to Ask Vendors

- Security program: documented policies, dedicated security personnel, certifications (SOC 2, ISO 27001), recent audits, employee training
- Data protection: what data is accessed, where stored, encryption at rest and in transit, who can access it, retention and deletion policies
- Access control: how access is controlled, MFA requirements, privileged access management, offboarding process
- Incident response: existence of a plan, breach notification timelines, past incidents and response
- Business continuity: backup procedures, recovery speed, disaster recovery plan and testing
- Vendor's own vendors: whether subcontractors are used and how their security is assured

Verifying Vendor Security Updates

Ask about update frequency, notification of security updates, automatic vs. manual updates, testing before release, and end-of-life policies. Maintain a list of vendor products and monitor their security advisories.

Support, Documentation, and Backup Responsibilities

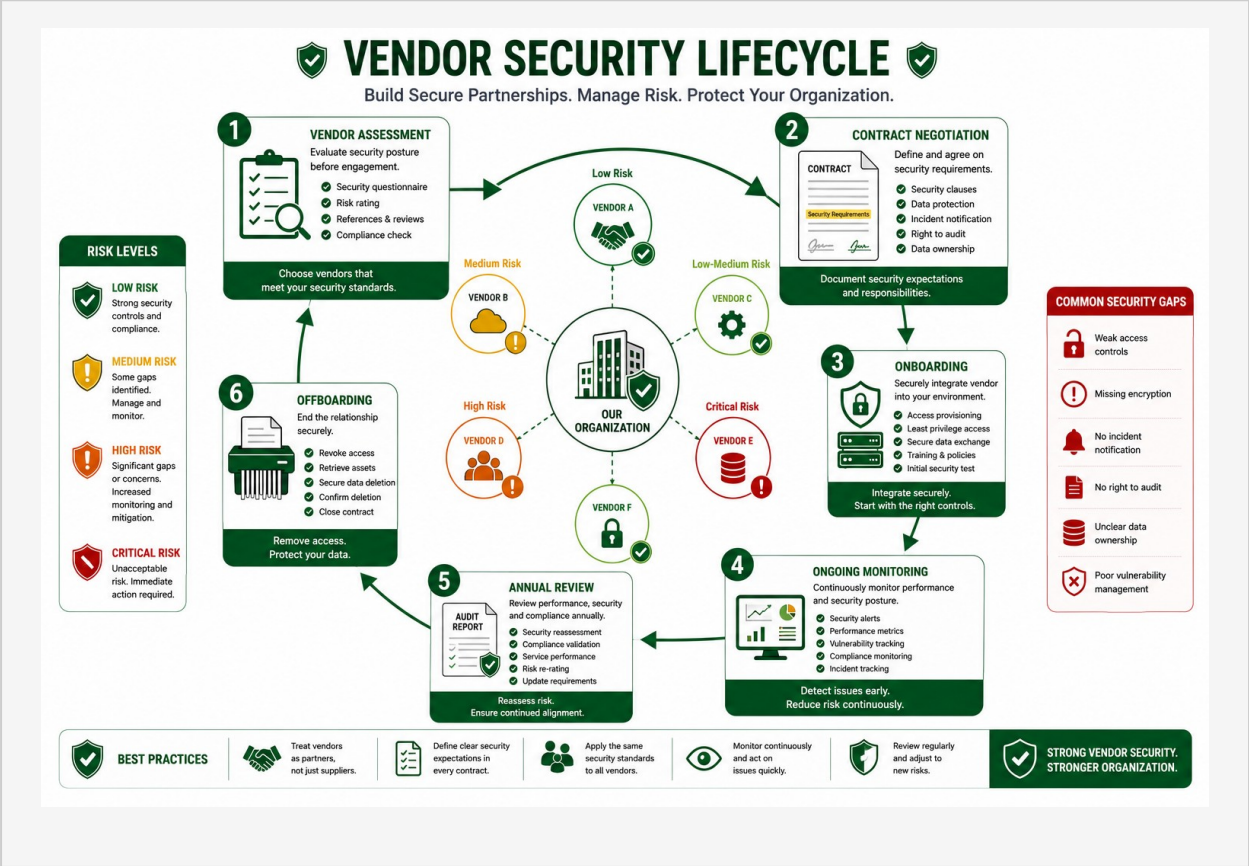
Assess support availability, channels, response times, and quality; request security documentation, configuration guides, and emergency contacts. Clarify who performs backups, frequency, retention, testing, your access to your own backups, and backup security—many vendors protect against disaster but not accidental or malicious deletion, so consider your own independent backups of vendor-hosted data.

Contracts, SLAs, and Ongoing Management

Contracts should address security requirements, data protection, breach notification, audit rights, data ownership and deletion, liability, and insurance. SLAs should define availability, performance, support response times, and remedies. Have contracts reviewed by legal counsel for critical vendors.

Ongoing management includes annual security reviews, monitoring vendor incidents, reviewing audit reports, periodic relationship reviews, and risk-rating vendors to focus effort on the highest-

risk relationships.



PART EIGHT

Preparing for Incidents

Incident response and business continuity

Incident Response

Security incidents will occur despite prevention efforts. How organizations respond determines whether they face minor disruptions or catastrophic failures. Effective response requires planning, clear procedures, defined roles, and regular practice.

What Constitutes a Security Incident

Any event compromising or threatening confidentiality, integrity, or availability: malware infections, ransomware, phishing-based compromise, unauthorized access, data breaches, denial of service, lost devices, insider threats, physical breaches, and vendor incidents.

The Five-Step Incident Response Framework

1. Identify

Detect and confirm an incident through user reports, security alerts, system monitoring, or external notification. Conduct an initial assessment and begin documentation immediately.

2. Contain

Isolate affected systems from the network, disable compromised accounts, block malicious traffic, and preserve evidence rather than deleting or wiping systems. Balance containment against operational needs and document all actions taken.

3. Notify

Internally: management immediately, IT/security staff, affected departments, and legal counsel for significant incidents. Externally: law enforcement (local police, Canadian Anti-Fraud Centre) for criminal activity, regulators within required timeframes, affected individuals for personal information breaches, customers/partners, and your cyber insurance provider. Be factual, avoid speculation, designate a single spokesperson, and document all communications.

4. Recover

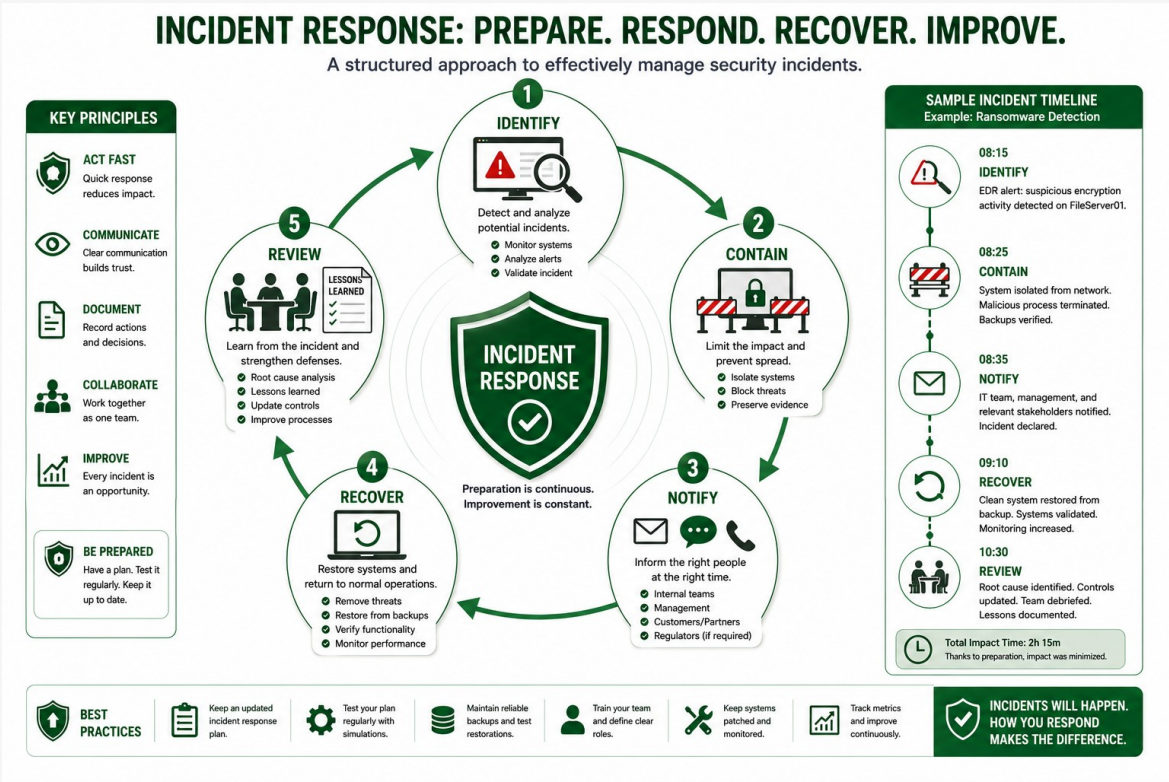
Eradicate the threat completely before restoring, restore from clean backups, consider rebuilding severely compromised systems from scratch, reset all potentially compromised credentials, apply security updates, verify system integrity, and restore gradually while monitoring.

5. Review

Conduct a post-incident review meeting, document the incident timeline, analyze root causes, evaluate response effectiveness, identify lessons learned, develop action items with owners and deadlines, update procedures, and follow up to ensure completion.

Incident Response Planning

A written plan should define roles and responsibilities, maintain current contact information for the response team and external resources, establish escalation procedures, prepare communication templates, and document technical procedures for common incident types. Test plans through tabletop exercises that walk through scenarios and identify gaps before a real incident occurs.


INCIDENT RESPONSE: PREPARE. RESPOND. RECOVER. IMPROVE.
A structured approach to effectively manage security incidents.
KEY PRINCIPLES
ACT FAST
Quick response reduces impact.
COMMUNICATE
Clear communication builds trust.
DOCUMENT
Record actions and decisions.
COLLABORATE
Work together as one team.
IMPROVE
Every incident is an opportunity.
BE PREPARED
Have a plan. Test it regularly. Keep it up to date.
1
IDENTIFY
Detect and analyze potential incidents.
Monitor systems
Analyze alerts
Validate incident
2
CONTAIN
Limit the impact and prevent spread.
Isolate systems
Block threats
Preserve evidence
3
NOTIFY
Inform the right people at the right time.
Internal teams
Management
Customers/Partners
Regulators (if required)
4
RECOVER
Restore systems and return to normal operations.
Remove threats
Restore from backups
Verify functionality
Monitor performance
5
REVIEW
LESSONS LEARNED
Learn from the incident and strengthen defenses.
Root cause analysis
Lessons learned
Update controls
Improve processes
INCIDENT RESPONSE
Preparation is continuous.
Improvement is constant.
SAMPLE INCIDENT TIMELINE
Example: Ransomware Detection
08:15
IDENTIFY
EDR alert: suspicious encryption activity detected on FileServer01.
08:25
CONTAIN
System isolated from network. Malicious process terminated. Backups verified.
08:35
NOTIFY
IT team, management, and relevant stakeholders notified. Incident declared.
09:10
RECOVER
Clean system restored from backup. Systems validated. Monitoring increased.
10:30
REVIEW
Root cause identified. Controls updated. Team debriefed. Lessons documented.
Total Impact Time: 2h 15m
Thanks to preparation, impact was minimized.
BEST PRACTICES
Keep an updated incident response plan.
Test your plan regularly with simulations.
Maintain reliable backups and test restorations.
Train your team and define clear roles.
Keep systems patched and monitored.
Track metrics and improve continuously.
INCIDENTS WILL HAPPEN. HOW YOU RESPOND MAKES THE DIFFERENCE.

Business Continuity

Business continuity is the capability to maintain or rapidly resume critical operations during and after disruptions—complementing incident response's focus on security events with broader resilience against any disruption.

Understanding Business Continuity

Business continuity focuses on maintaining operations through manual workarounds and alternative processes; disaster recovery focuses specifically on restoring IT systems. Small organizations are often more vulnerable to disruptions than large ones because they have fewer resources and less redundancy.

Common disruptions requiring continuity planning: ransomware, hardware failures, internet/telecom outages, power outages, natural disasters, facility access issues, key personnel unavailability, and vendor failures.

Identifying Critical Business Functions

List all business functions, assess criticality (speed of resumption needed, impact of unavailability, dependencies), and prioritize as Critical (hours), Important (days), or Normal (weeks). For each critical function, identify required systems, information, people, vendors, and facilities.

Manual Procedures and Workarounds

Document current technology-dependent processes and identify manual alternatives with step-by-step instructions, required resources, roles, and quality controls. Examples: paper order forms if systems are down, printed customer lists, manual payment imprinters, or phone trees if email is unavailable. Manual procedures are temporary measures, not permanent solutions.

Alternative Communications

Identify alternatives to email, phone systems, and collaboration platforms: personal email accounts (with understood limitations), mobile phones, phone trees, alternative collaboration platforms, social media, and physical gathering locations. Maintain current contact lists, define communication priorities and protocols, and plan for regular updates during extended disruptions.

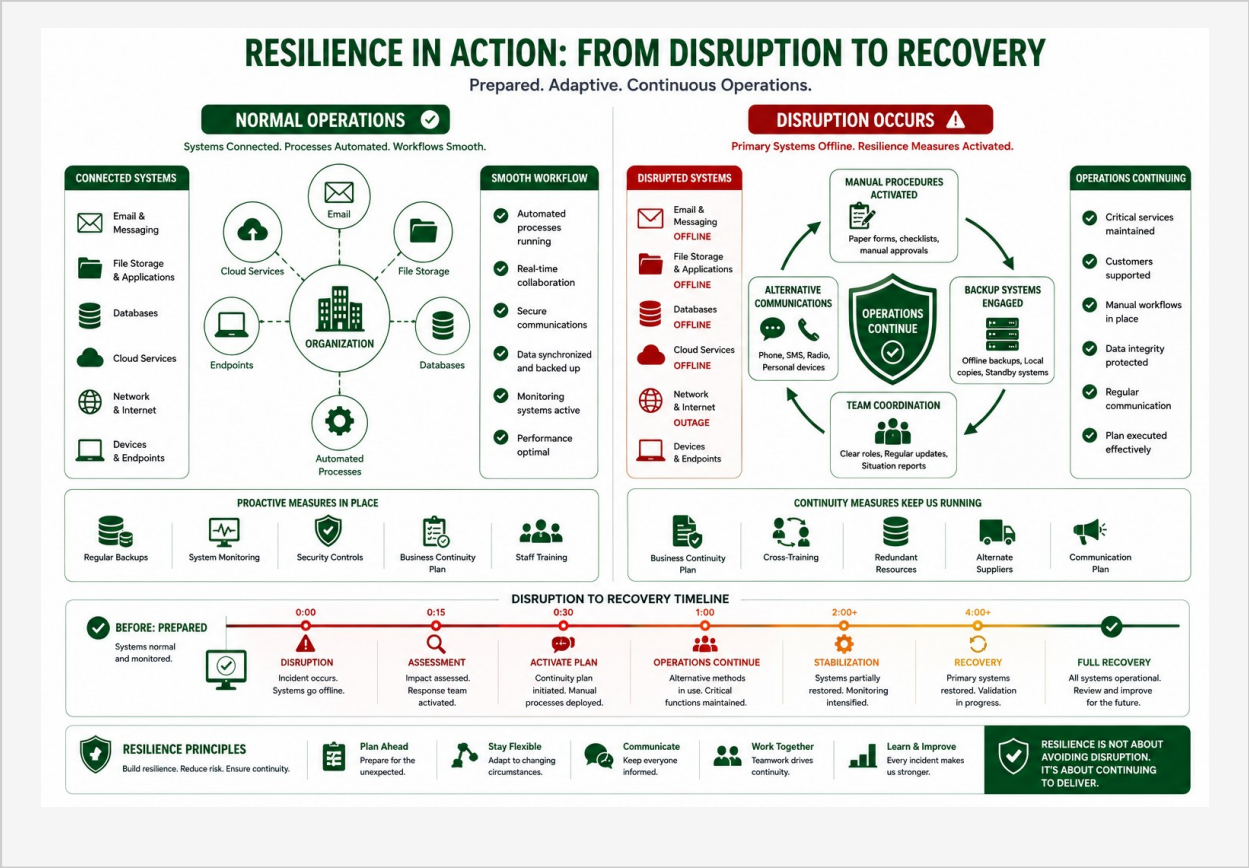
Backup Systems, Redundancy, and Recovery Objectives

Consider backup internet connections, backup power (UPS, generators), spare equipment, and cloud-based alternatives, weighing cost against the cost of downtime. Define Recovery Time Objectives (maximum acceptable downtime) and Recovery Point Objectives (maximum acceptable data loss) for each system, which inform backup frequency and redundancy investments.

Documentation and Testing

Document critical functions, RTOs/RPOs, manual procedures, alternative communications, backup activation procedures, roles, and vendor contacts. Keep plans accessible in printed form, on

portable storage, and in cloud storage. Review annually and after any disruption. Test through tabletop exercises annually, functional tests of specific elements, and periodic full simulations.



PART NINE

Policy and Culture

Policies, training, habits, and dispelling common myths

Security Policies

Security policies establish organizational expectations, requirements, and procedures. Effective policies for small organizations are clear, practical, relevant, accessible, and treated as living documents rather than lengthy, complex documents.

Acceptable Use Policy

Defines authorized use, prohibited activities (bypassing controls, sharing credentials, unauthorized software, inappropriate content), internet/email/social media use, monitoring notice, and consequences for violations.

Password Policy

Minimum length (12+ standard, 20+ administrative), uniqueness across systems, password manager use, prohibition on sharing or writing down passwords insecurely, password change triggers (compromise, role change—not arbitrary schedules), and MFA requirements for remote access, sensitive systems, and administrative accounts.

Remote Work Policy

Approved and prohibited locations; device security (organizational or approved personal devices, encryption, screen locks, updates); network security (VPN, secure home Wi-Fi, no public Wi-Fi without VPN); physical security; and communication security.

Mobile Device Policy

Device requirements and minimum OS versions; security requirements (screen locks, passcodes, encryption, updates); application restrictions (approved apps, no jailbreaking); lost/stolen device reporting and remote wipe; and BYOD considerations for personal devices.

Backup Policy

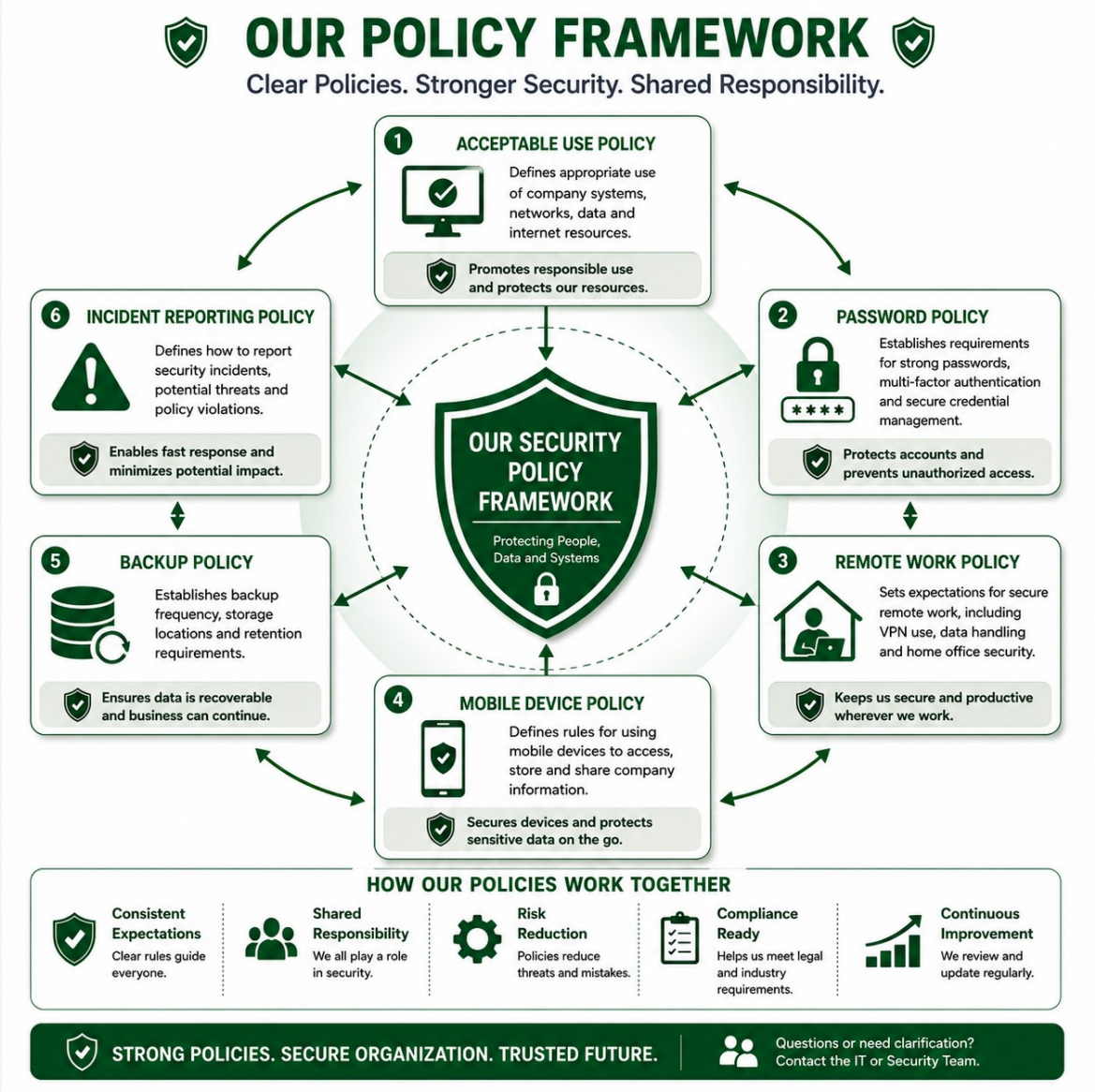
Scope (all organizational data, configurations, applications, email); frequency by data criticality; retention periods; storage requirements (3-2-1 rule, offsite, offline/immutable); testing requirements; and backup encryption and access controls.

Incident Reporting Policy

What to report (malware, phishing, lost devices, unauthorized access, breaches, unusual behavior, concerns); how and when to report (immediately, even if unsure); and an emphasized no-blame culture where reporting is valued, not punished.

Policy Implementation and Maintenance

Ensure management approval, communicate to all employees (including onboarding), provide training, make policies accessible, and consider requiring acknowledgment. Review annually, update as technologies and threats change, maintain version control, and communicate changes clearly.


OUR POLICY FRAMEWORK
Clear Policies. Stronger Security. Shared Responsibility.
1 ACCEPTABLE USE POLICY
Defines appropriate use of company systems, networks, data and internet resources.
Promotes responsible use and protects our resources.
2 PASSWORD POLICY
Establishes requirements for strong passwords, multi-factor authentication and secure credential management.
Protects accounts and prevents unauthorized access.
3 REMOTE WORK POLICY
Sets expectations for secure remote work, including VPN use, data handling and home office security.
Keeps us secure and productive wherever we work.
4 MOBILE DEVICE POLICY
Defines rules for using mobile devices to access, store and share company information.
Secures devices and protects sensitive data on the go.
5 BACKUP POLICY
Establishes backup frequency, storage locations and retention requirements.
Ensures data is recoverable and business can continue.
6 INCIDENT REPORTING POLICY
Defines how to report security incidents, potential threats and policy violations.
Enables fast response and minimizes potential impact.
OUR SECURITY POLICY FRAMEWORK
Protecting People, Data and Systems
HOW OUR POLICIES WORK TOGETHER
Consistent Expectations
Clear rules guide everyone.
Shared Responsibility
We all play a role in security.
Risk Reduction
Policies reduce threats and mistakes.
Compliance Ready
Helps us meet legal and industry requirements.
Continuous Improvement
We review and update regularly.
STRONG POLICIES. SECURE ORGANIZATION. TRUSTED FUTURE.
Questions or need clarification? Contact the IT or Security Team.

Employee Awareness and Training

Technology alone cannot protect organizations—people must understand security risks and their role in protecting information. Effective awareness programs are ongoing, engaging, and practical.

Why Security Awareness Training Matters

Human factors contribute to the majority of security incidents. Trained employees recognize and avoid threats, enable early detection through reporting, reinforce a shared security culture, demonstrate organizational due diligence, and gain confidence to make security-conscious decisions.

Initial Security Training

All new employees should receive training covering security policies, password security and managers, email security and phishing recognition, physical security, incident reporting, and information handling. Typically 30-60 minutes, delivered in-person, online, or a combination, kept concise and immediately applicable.

Ongoing Security Awareness

Monthly reminders

Brief email tips, newsletter articles, posters, or intranet content covering one topic per month—for example, passwords in January, phishing in February, mobile devices in March, and so on through the year, culminating in Cybersecurity Awareness Month activities in October.

Quarterly training sessions

15-30 minute interactive sessions covering phishing, passwords/MFA, mobile/remote work, and incident response/continuity in rotation, using real (anonymized) examples relevant to your organization.

Simulated phishing exercises

Test awareness with safe simulated emails, starting simple and increasing difficulty, focusing on education rather than punishment, providing immediate feedback, and tracking organizational trends rather than individual blame.

Encouraging Incident Reporting

Remove barriers through a no-blame culture, easy reporting processes, timely acknowledgment, positive reinforcement, and leadership modeling. Employees should report suspicious emails, unusual behavior, lost devices, suspected malware, unauthorized access, physical security concerns, vendor issues, or anything that "doesn't feel right," through multiple accessible, monitored channels.


Security Awareness: Transforming Employees Into Active Defenders.
Knowledge. Awareness. Action. Together, we keep our organization secure.
SECURITY IS EVERYONE'S RESPONSIBILITY
See something
Say something
Do something
PHISHING EMAIL EXAMPLES – CAN YOU SPOT THE RED FLAGS?
SUSPICIOUS EMAIL
LEGITIMATE EMAIL
WHEN IN DOUBT, STOP. VERIFY. REPORT.
STRONG PASSWORDS
Long. Unique. Never Shared.
REPORT SUSPICIOUS ACTIVITY
See it. Report it. Stop it.
PROTECT OUR DATA
Classify, Handle, Protect.
TOGETHER WE STAY SECURE
We all play a role in keeping our organization safe.
TODAY'S AGENDA
Why Security Matters
Phishing Awareness
Password Best Practices
Data Protection
How to Report Incidents
Q & A
SECURITY STARTS WITH YOU
Think Before You Click
Protect Our Data
Report Suspicious Activity
Keep Our Organization Safe
THINK BEFORE YOU CLICK!
SECURITY AWARENESS WORKBOOK
Knowledge Protects. Awareness Empowers.
COMMON THREATS
Phishing
Malware
Ransomware
Social Engineering
GOOD SECURITY HABITS
Use Strong Passwords
Enable Multi-Factor Authentication
Keep Software Updated
Lock Your Devices
Report Incidents
OUR CORE SECURITY BEHAVIORS
THINK
Stay alert and question unusual requests.
VERIFY
Check before you click or share.
PROTECT
Follow policies and safeguard information.
REPORT
Report suspicious activity right away.
SUPPORT
Look out for each other and share knowledge.
TOGETHER, WE BUILD A CULTURE OF SECURITY AND RESILIENCE.

Security Habits Checklist

Cybersecurity is built through consistent habits practiced daily, weekly, monthly, quarterly, and annually—not through one-time projects.

Daily Habits

All employees: lock your screen when away, think before clicking links, check for HTTPS before entering sensitive information, secure documents, report suspicious activity immediately, use your password manager, and verify unusual requests through a secondary channel.

Managers: review unusual access or permission changes and model good behavior. IT staff: review alerts and logs, monitor backup completion, and check for critical updates.

Weekly Habits

All employees: review the password manager for weak/reused passwords, check device updates, verify mobile backups, clear unnecessary files, and review recent account activity.

Managers: review team access permissions and confirm departing employees' access was removed. IT staff: review backup logs, check for updates, review account activity, test one backup restoration, and review security logs.

Monthly Habits

All employees: update emergency contacts, check credit reports, review cloud service privacy settings, and verify device encryption.

IT staff and security coordinators: remove inactive accounts, verify current updates across systems, test disaster recovery for one system, review documentation and security metrics, review vendor patches, and conduct vulnerability scanning if available.

Quarterly Habits

All employees attend quarterly training and review policies. IT staff conduct comprehensive security assessments, test complete disaster recovery, review vendor assessments, conduct comprehensive backup restoration tests, and update incident response procedures. Leadership reviews security posture, budget, and conducts a tabletop exercise.

Annual Habits

Conduct the comprehensive Security Self-Assessment, review and update all policies, conduct a full disaster recovery test, review business continuity plans, assess all vendor security practices, conduct comprehensive employee training, review physical security and insurance coverage, assess regulatory compliance, and consider a penetration test or security audit.

Making Security Habits Stick

Start small and build gradually, use calendar reminders, clearly assign responsibility, track completion with simple checklists, regularly review and adjust, and celebrate consistent success. Consistency matters more than perfection.


SECURITY HABITS
BUILDING RESILIENCE THROUGH CONSISTENT PRACTICE.
DAILY
Check for phishing emails
Verify requests before acting
Use strong passwords and MFA
Lock devices when away
Report suspicious activity
WEEKLY
Review security alerts
Update software and apps
Backup important files
Review user access and permissions
Validate security habits with your team
MONTHLY
Review and test backup systems
Check device and disk health
Review and update security policies
Audit admin and user accounts
Run vulnerability scans
QUARTERLY
Review security training completion
Test incident response plan
Review third-party and vendor access
Assess and update risk register
Conduct security awareness refreshers
ANNUAL
Perform full security program review
Conduct penetration testing
Update business continuity plan
Review and renew policies and contracts
Evaluate tools and technologies
Backup Status
Successful
RISK ASSESSMENT
SECURITY REVIEW
Small habits. Big impact. Stronger together.
Consistency today. Resilience tomorrow.

Cybersecurity Myths vs. Reality

Misconceptions lead organizations to make poor security decisions, misallocate resources, or develop false confidence in inadequate protections.

Myth: "My antivirus software protects everything."

Reality: Antivirus is one important layer, but cannot stop phishing, social engineering, insider threats, configuration errors, or secure cloud services on its own. Effective security requires multiple layers.

Myth: "My business is too small to be targeted."

Reality: Automated attacks don't discriminate by size; small organizations are often easier targets, hold valuable data, and are used as supply-chain footholds to larger partners.

Myth: "Backups mean I'm completely safe."

Reality: Ransomware specifically targets backups; backups don't prevent data theft, take time to restore, may be incomplete, and often fail when untested. Backups are essential but must be part of a comprehensive strategy including prevention, detection, and response.

Myth: "Cybersecurity is too expensive for small organizations."

Reality: Many effective controls—strong passwords, MFA, updates, training—cost little or nothing. Cloud services include built-in security features, and incidents are typically far more expensive than reasonable prevention.

Myth: "We don't have anything worth stealing."

Reality: Every organization has valuable customer information, financial data, credentials, business information, and computing resources worth protecting. If you use computers or store information, you have something worth protecting.

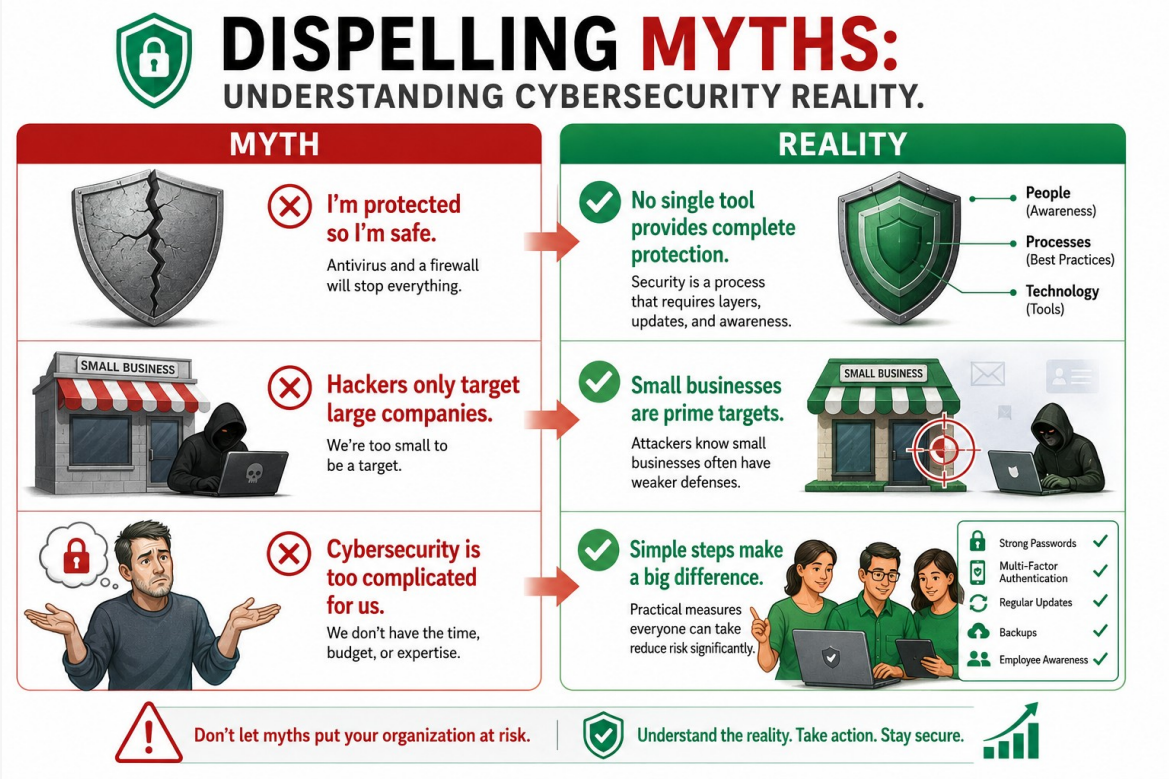
Myth: "Security and usability are opposites."

Reality: Well-designed security can improve usability—password managers, single sign-on, and automatic updates reduce friction while improving protection. Poor security implementations, not security itself, create usability problems.

Myth: "Compliance means we're secure."

Reality: Compliance establishes a minimum, point-in-time baseline addressing specific requirements, not comprehensive, continuous security. View compliance as a starting point, not an endpoint.

Effective security is built on realistic understanding of threats, honest assessment of capabilities, and consistent implementation of fundamental practices—not expensive products or wishful thinking.


DISPELLING MYTHS:
UNDERSTANDING CYBERSECURITY REALITY.
MYTH
REALITY
I'm protected so I'm safe.
Antivirus and a firewall will stop everything.
No single tool provides complete protection.
Security is a process that requires layers, updates, and awareness.
People (Awareness)
Processes (Best Practices)
Technology (Tools)
SMALL BUSINESS
Hackers only target large companies.
We're too small to be a target.
Small businesses are prime targets.
Attackers know small businesses often have weaker defenses.
SMALL BUSINESS
Cybersecurity is too complicated for us.
We don't have the time, budget, or expertise.
Simple steps make a big difference.
Practical measures everyone can take reduce risk significantly.
Strong Passwords
Multi-Factor Authentication
Regular Updates
Backups
Employee Awareness
Don't let myths put your organization at risk.
Understand the reality. Take action. Stay secure.

PART TEN

Planning and Resources

A roadmap, self-assessment, further resources, and a quick reference card

First 30, 90, and 365 Days Action Roadmap

Improving cybersecurity can feel overwhelming. This roadmap provides a phased approach starting with essential foundations and progressing to comprehensive security maturity.

First 30 Days: Essential Foundations

Week 1: Assessment and awareness

Complete the Security Self-Assessment; establish incident reporting contacts and procedures; communicate security priorities to all employees.

Week 2: Authentication and access

Establish password requirements (12+ characters, uniqueness); deploy a password manager to all employees; enable MFA on critical accounts (email, financial, admin).

Week 3: Backups and updates

Verify current backups, test one restoration, implement the 3-2-1 rule with an offline/immutable copy; enable automatic updates on workstations and servers where appropriate.

Week 4: Policies and physical security

Document acceptable use, password, incident reporting, and remote work policies; implement clean desk practices; verify doors lock properly; review and plan next steps.

First 90 Days: Core Implementations

Days 31-45: Email and communication

Implement email filtering and authentication (SPF/DKIM/DMARC); train employees on phishing recognition; run the first simulated phishing exercise; establish secure file sharing.

Days 46-60: Mobile and remote work

Establish mobile device policy with screen locks, encryption, and remote wipe; implement VPN for remote access; train employees on remote work security.

Days 61-75: Vendors

Inventory vendors with system/data access; assess critical vendor security practices; review contracts for security requirements; document vendor incident contacts.

Days 76-90: Monitoring and response

Implement basic security monitoring; develop an incident response plan and team; conduct a tabletop exercise; review progress and plan the next nine months.

First 365 Days: Continuous Improvement and Maturity

Months 4-6: Awareness and culture

Implement monthly reminders, quarterly training, and regular simulated phishing; integrate security into regular business processes and recognize good practices.

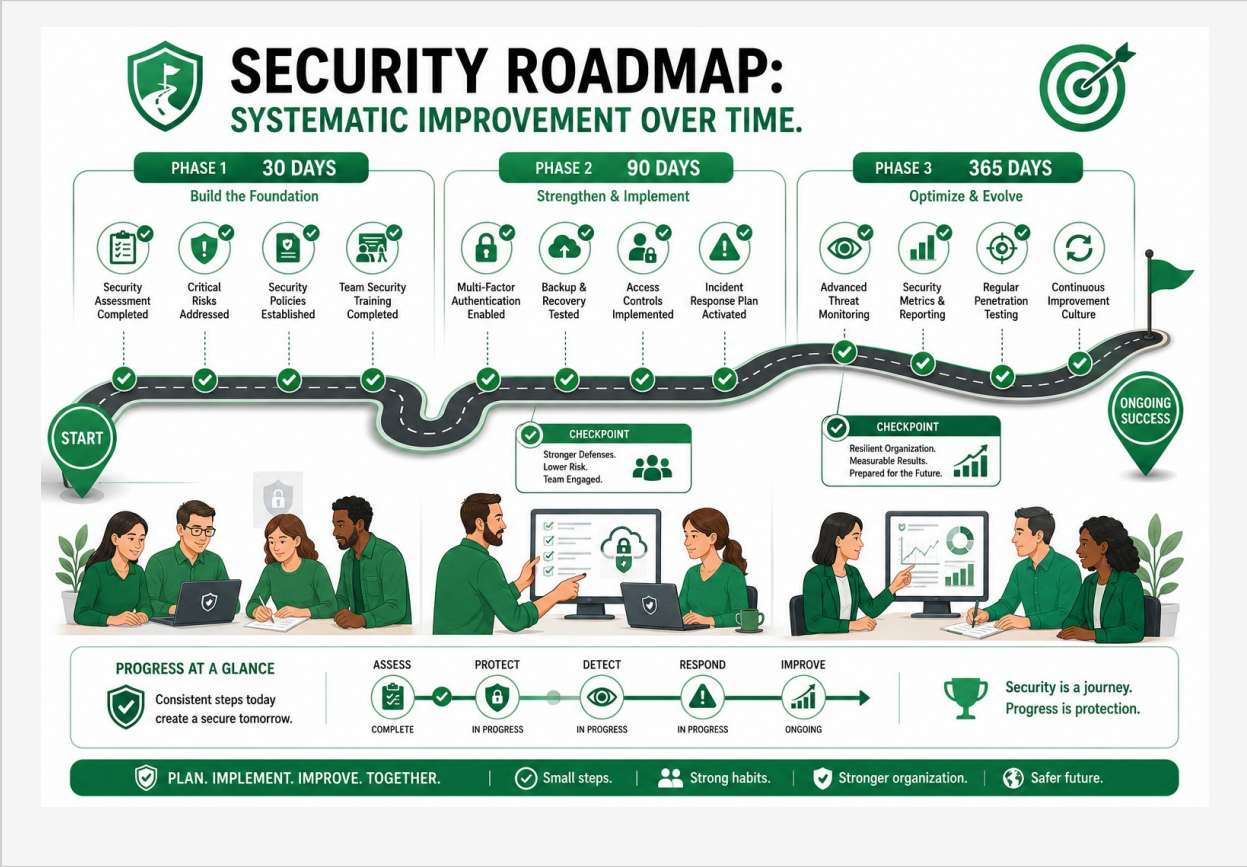
Months 7-9: Advanced controls and testing

Implement network segmentation and enhanced logging where appropriate; conduct comprehensive backup restoration and disaster recovery tests; consider vulnerability scanning or penetration testing.

Months 10-12: Continuity and compliance

Develop a comprehensive business continuity plan; test it; review compliance with applicable regulations; conduct a comprehensive annual security audit and plan priorities for year two.

Adapt this roadmap to your organization's context—focus on progress, not perfection, and measure progress with the Security Self-Assessment at 30, 90, and 365 days.



Security Self-Assessment

This self-assessment evaluates your cybersecurity posture across 20 critical areas using traffic-light scoring: Green (implemented effectively), Yellow (partially implemented), Red (not implemented or urgent).

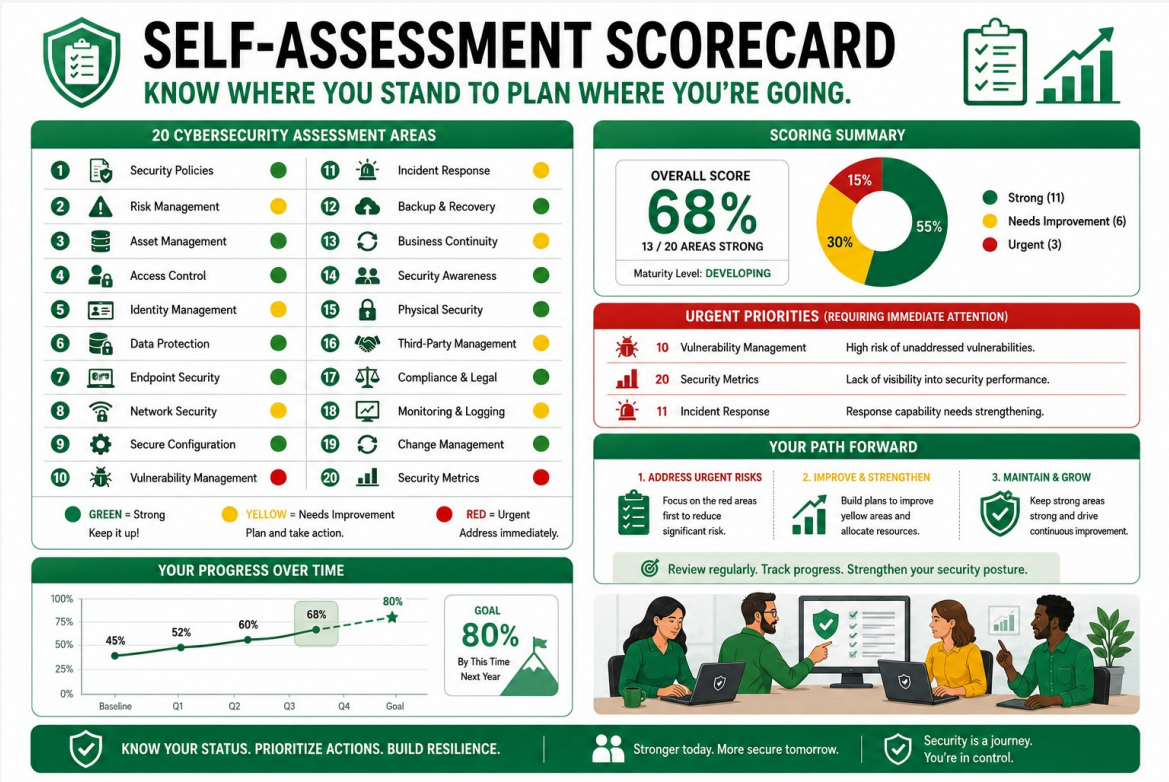
Assessment Areas

- 1. Password security – strong, unique passwords managed with a password manager
- 2. Multi-factor authentication – enabled on all critical accounts
- 3. Software updates – systems patched promptly, automatic updates where possible
- 4. Backups – follow the 3-2-1 rule, include offline/immutable copies, tested regularly
- 5. Email security – phishing recognition, verification procedures, filtering in place
- 6. Incident response – documented procedures, trained team, regularly tested
- 7. Access control – least privilege enforced, regular access reviews
- 8. Physical security – locked doors, clean desk policy, secured server rooms
- 9. Mobile device security – encrypted, screen-locked, remote wipe enabled
- 10. Remote work security – VPN required, policy and training in place
- 11. Vendor security – assessed, contractual requirements, ongoing monitoring
- 12. Security awareness training – initial and ongoing, simulated exercises
- 13. Security policies – documented, comprehensive, regularly reviewed
- 14. Business continuity – documented plan, manual procedures, tested
- 15. Data classification – formal system with appropriate protections
- 16. Encryption – comprehensive for data at rest and in transit
- 17. Network security – segmented, firewalled, strong Wi-Fi, monitored
- 18. Account management – prompt offboarding, no shared accounts, accurate inventory
- 19. Security monitoring – active monitoring, regular log review, tracked metrics
- 20. Continuous improvement – regular assessment, lessons learned, tracked progress

Scoring and Next Steps

Count your Green, Yellow, and Red scores. 16-20 Green: excellent posture—maintain and continuously improve. 11-15 Green: good foundation—prioritize yellow and red areas. 6-10 Green: moderate posture—significant improvement needed; use the roadmap to prioritize. 0-5 Green: urgent action required—begin with First 30 Days priorities immediately.

Conduct this assessment quarterly to track improvement and identify new priorities. Honest assessment is more valuable than optimistic scoring.


SELF-ASSESSMENT SCORECARD
KNOW WHERE YOU STAND TO PLAN WHERE YOU'RE GOING.
20 CYBERSECURITY ASSESSMENT AREAS
1 Security Policies
2 Risk Management
3 Asset Management
4 Access Control
5 Identity Management
6 Data Protection
7 Endpoint Security
8 Network Security
9 Secure Configuration
10 Vulnerability Management
11 Incident Response
12 Backup & Recovery
13 Business Continuity
14 Security Awareness
15 Physical Security
16 Third-Party Management
17 Compliance & Legal
18 Monitoring & Logging
19 Change Management
20 Security Metrics
GREEN = Strong
Keep it up!
YELLOW = Needs Improvement
Plan and take action.
RED = Urgent
Address immediately.
SCORING SUMMARY
OVERALL SCORE
68%
13 / 20 AREAS STRONG
Maturity Level: DEVELOPING
15%
55%
30%
Strong (11)
Needs Improvement (6)
Urgent (3)
URGENT PRIORITIES (REQUIRING IMMEDIATE ATTENTION)
10 Vulnerability Management
High risk of unaddressed vulnerabilities.
20 Security Metrics
Lack of visibility into security performance.
11 Incident Response
Response capability needs strengthening.
YOUR PATH FORWARD
1. ADDRESS URGENT RISKS
Focus on the red areas first to reduce significant risk.
2. IMPROVE & STRENGTHEN
Build plans to improve yellow areas and allocate resources.
3. MAINTAIN & GROW
Keep strong areas strong and drive continuous improvement.
Review regularly. Track progress. Strengthen your security posture.
YOUR PROGRESS OVER TIME
100%
75%
50%
25%
0%
45%
52%
60%
68%
80%
Baseline
Q1
Q2
Q3
Q4
Goal
GOAL
80%
By This Time Next Year
KNOW YOUR STATUS. PRIORITIZE ACTIONS. BUILD RESILIENCE.
Stronger today. More secure tomorrow.
Security is a journey. You're in control.

Where to Learn More

Cybersecurity is a continuously evolving field. The following authoritative resources support ongoing education.

Canadian Resources

Canadian Centre for Cyber Security (cyber.gc.ca): Baseline Cyber Security Controls for Small and Medium Organizations, threat bulletins, awareness materials, and incident reporting. Office of the Privacy Commissioner of Canada (priv.gc.ca): privacy legislation guidance, breach reporting requirements, and best practices.

International Resources

CISA (cisa.gov): cybersecurity best practices, alerts and advisories, free vulnerability scanning services, and a small-business Cyber Essentials starter kit. NIST (nist.gov/cybersecurity): the NIST Cybersecurity Framework and a Small Business Cybersecurity Corner.

Vulnerability and Threat Intelligence

CVE (cve.org): standardized identifiers for known vulnerabilities. NVD (nvd.nist.gov): detailed vulnerability analysis, severity scoring, and remediation guidance.

Linux and Open Source Security

Ubuntu Security (security.ubuntu.com), Debian Security (debian.org/security), Red Hat Security (access.redhat.com/security), and SUSE Security (suse.com/security) each provide advisories and best practices. The Open Source Security Foundation (openssf.org) works to improve open source security through collaboration.

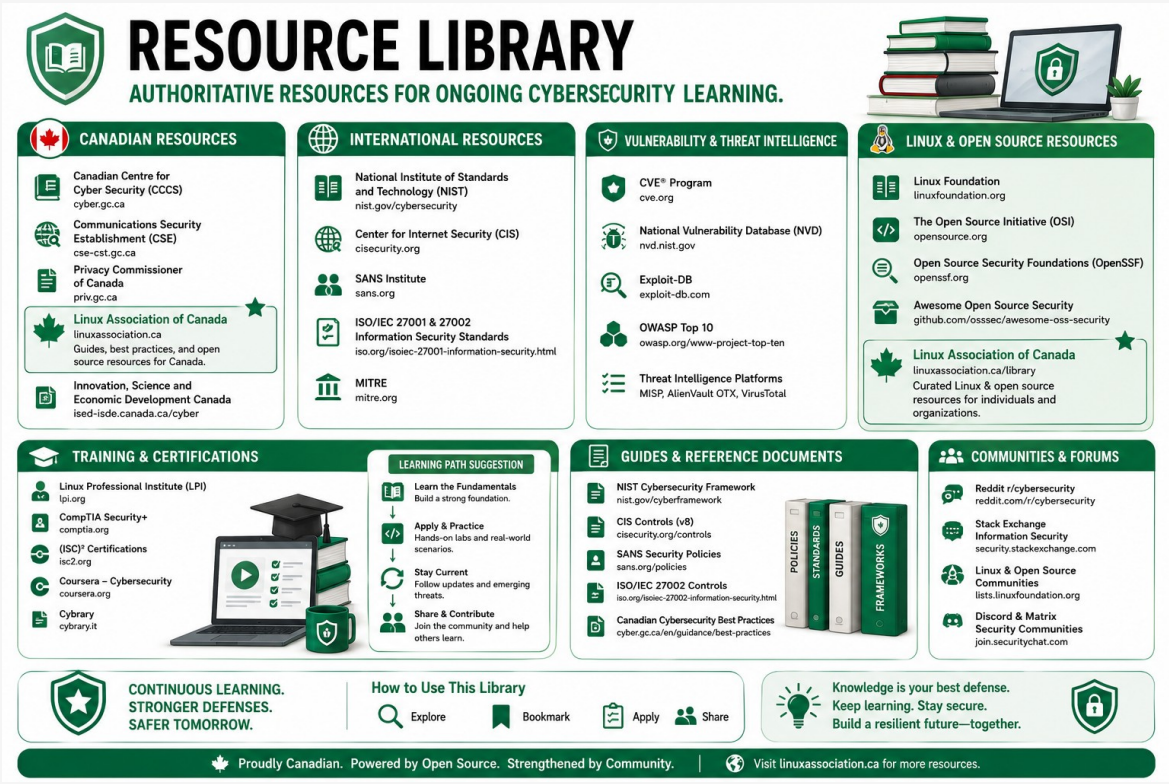
Security News and Training

Krebs on Security, Bleeping Computer, The Hacker News, and Dark Reading provide ongoing threat coverage. SANS Cyber Aces, Cybrary, Coursera, and edX offer free and paid cybersecurity training.

Linux Association of Canada Resources

Cybersecurity awareness and training materials, Linux and open source security guidance, community forums, and school/youth outreach programs. All companion resources for this guide —policy templates, incident response and business continuity templates, assessment worksheets, training materials, and posters—are available at linuxassociation.ca/resources.

Contact: linuxassociation.ca • info@linuxassociation.ca


RESOURCE LIBRARY
AUTHORITATIVE RESOURCES FOR ONGOING CYBERSECURITY LEARNING.
CANADIAN RESOURCES
Canadian Centre for Cyber Security (CCCS)
cyber.gc.ca
Communications Security Establishment (CSE)
cse-cst.gc.ca
Privacy Commissioner of Canada
priv.gc.ca
Linux Association of Canada
linuxassociation.ca
Guides, best practices, and open source resources for Canada.
Innovation, Science and Economic Development Canada
ised-isde.canada.ca/cyber
INTERNATIONAL RESOURCES
National Institute of Standards and Technology (NIST)
nist.gov/cybersecurity
Center for Internet Security (CIS)
cisecurity.org
SANS Institute
sans.org
ISO/IEC 27001 & 27002 Information Security Standards
iso.org/isoiec-27001-information-security.html
MITRE
mitre.org
VULNERABILITY & THREAT INTELLIGENCE
CVE® Program
cve.org
National Vulnerability Database (NVD)
nvd.nist.gov
Exploit-DB
exploit-db.com
OWASP Top 10
owasp.org/www-project-top-ten
Threat Intelligence Platforms
MISP, AlienVault OTX, VirusTotal
LINUX & OPEN SOURCE RESOURCES
Linux Foundation
linuxfoundation.org
The Open Source Initiative (OSI)
opensource.org
Open Source Security Foundations (OpenSSF)
openssf.org
Awesome Open Source Security
github.com/osssec/awesome-oss-security
Linux Association of Canada
linuxassociation.ca/library
Curated Linux & open source resources for individuals and organizations.
TRAINING & CERTIFICATIONS
Linux Professional Institute (LPI)
lpi.org
CompTIA Security+
comptia.org
(ISC)² Certifications
isc2.org
Coursera – Cybersecurity
coursera.org
Cybrary
cybrary.it
LEARNING PATH SUGGESTION
Learn the Fundamentals
Build a strong foundation.
Apply & Practice
Hands-on labs and real-world scenarios.
Stay Current
Follow updates and emerging threats.
Share & Contribute
Join the community and help others learn.
GUIDES & REFERENCE DOCUMENTS
NIST Cybersecurity Framework
nist.gov/cyberframework
CIS Controls (v8)
cisecurity.org/controls
SANS Security Policies
sans.org/policies
ISO/IEC 27002 Controls
iso.org/isoiec-27002-information-security.html
Canadian Cybersecurity Best Practices
cyber.gc.ca/en/guidance/best-practices
POLICIES
STANDARDS
GUIDES
FRAMEWORKS
COMMUNITIES & FORUMS
Reddit r/cybersecurity
reddit.com/r/cybersecurity
Stack Exchange Information Security
security.stackexchange.com
Linux & Open Source Communities
lists.linuxfoundation.org
Discord & Matrix Security Communities
join.securitychat.com
CONTINUOUS LEARNING.
STRONGER DEFENSES.
SAFER TOMORROW.
How to Use This Library
Explore
Bookmark
Apply
Share
Knowledge is your best defense.
Keep learning. Stay secure.
Build a resilient future—together.
Proudly Canadian. Powered by Open Source. Strengthened by Community.
Visit linuxassociation.ca for more resources.

Cybersecurity Quick Reference Card

Keep this reference accessible for quick action during security incidents.

If You Suspect a Security Incident

1. Disconnect (if appropriate)

Disconnect from the network if you see active ransomware encryption, unauthorized access in progress, or spreading malware—unplug the network cable or turn off Wi-Fi, but do NOT shut down the computer, which preserves evidence. Don't disconnect just for a suspicious email; report it instead.

2. Report immediately

Contact IT support, the security team, or your manager. Describe what happened, when, what's affected, and what you've already done. Report even if you're unsure—false alarms are better than unreported incidents.

3. Preserve evidence

Do not delete files or emails, clear history, restart systems, or try to fix things yourself. Do leave systems as they are, take photos of errors, write down what happened, and save suspicious emails without clicking anything.

4. Call for support

Internal IT/security/management contacts; external IT provider, cyber insurance, and legal counsel; for criminal activity, local police, RCMP Cybercrime (1-800-771-5401), and the Canadian Anti-Fraud Centre (1-888-495-8501).

5. Don't panic

Incidents happen to all organizations. Quick reporting enables quick response. You won't be blamed for reporting—stay calm, follow instructions, and answer questions honestly.

Common Incident Types and Immediate Actions

- Suspicious email/phishing: don't click or reply; report; delete once instructed
- Ransomware: disconnect immediately; do not pay without consulting management and experts; report and preserve systems
- Lost or stolen device: report immediately with device details; IT remotely wipes if possible; change accessible account passwords
- Compromised account: change the password immediately, enable MFA, report, review activity
- Malware infection: disconnect, report, do not attempt removal yourself, preserve for investigation
- Unauthorized access: report immediately, change affected passwords, review logs, preserve evidence

Prevention Reminders

Daily: lock your screen, think before clicking, verify unusual requests, report suspicious activity.

Weekly: check for updates, review your password manager, verify backups. Monthly: attend training, review policies, update emergency contacts.

Remember: security is everyone's responsibility. When in doubt, report it.

QUICK REFERENCE:

YOUR EMERGENCY SECURITY RESPONSE GUIDE

Stay Calm. Act Fast. Report Immediately.

EMERGENCY CONTACTS

IT / Security Team
Phone: _____
Email: _____

Manager / Supervisor
Phone: _____
Email: _____

Incident Response Lead
Phone: _____
Email: _____

Legal / Privacy Officer
Phone: _____
Email: _____

Communications / PR
Phone: _____
Email: _____

911 **Emergency Services** (if needed)
Fire • Police • Ambulance

PREVENTION REMINDERS

- Keep software and systems updated.
- Use strong passwords and MFA.
- Be cautious of phishing emails and links.
- Lock your screen when away.
- Back up important data regularly.
- Report suspicious activity immediately.

SUSPECT A SECURITY INCIDENT?

DISCONNECT Isolate affected device/system from the network. →
REPORT Report immediately to IT/Security Team. →
DOCUMENT Record what you saw and what you did.

INCIDENT RESPONSE: STEP-BY-STEP

1. **IDENTIFY**
   Notice unusual activity or possible security incident.
   Trust your instincts and act.
2. **CONTAIN**
   Disconnect device from network.
   Do not power off unless instructed.
3. **REPORT**
   Contact IT/Security Team immediately.
   Provide details of what happened.
4. **PRESERVE**
   Do not delete files, emails, or logs.
   Do not make changes to affected system.
5. **COOPERATE**
   Follow instructions from the response team.
   Provide information and answer questions.
6. **RECOVER**
   Wait for clearance before reconnecting systems. Learn and improve.

WHAT TO REPORT

- ☑ Suspicious emails or messages
- ☑ Unusual system behavior
- ☑ Unauthorized access attempts
- ☑ Lost or stolen devices
- ☑ Data leaks or exposure
- ☑ Any security policy violations

INCIDENT SEVERITY GUIDE

CRITICAL (Red)	Active breach, data loss, system down, ransomware	**Call immediately!**
HIGH (Orange)	Suspicious activity, unauthorized access	**Report within 15 minutes.**
MEDIUM (Yellow)	Policy violation, malware alert, potential risk	**Report within 1 hour.**
LOW (Green)	Informational events, low-impact issues	**Report within 24 hours.**

QUICK CHECK: IS IT AN INCIDENT?

Is data possibly exposed or accessed by unauthorized people?	Yes	No
Is a system behaving unusually?	Yes	No
Did you receive a suspicious email, link or attachment?	Yes	No
Has a device been lost, stolen or compromised?	Yes	No
Are you unsure if something is safe or normal?	Yes	No

IF YOU ANSWERED YES TO ANY QUESTION:

REPORT IT.
ITS BETTER TO REPORT THAN REGRET.

IMPORTANT NOTES

Add your organization logo or sticker here

SECURITY IS EVERYONE'S RESPONSIBILITY. | BE PREPARED. STAY ALERT. KEEP EACH OTHER SAFE.

PART ELEVEN

Closing Thoughts

Final reflections and about the Linux Association of Canada

Final Thoughts

Effective cybersecurity is built on people who understand risks and report concerns, processes that establish clear expectations and enable quick response, technology that is kept updated and properly configured, and continuous improvement through regular assessment. Notice what's missing: expensive enterprise products and massive budgets. The primary investment required is attention and consistency.

Small Organizations Can Become Significantly More Resilient

Strong passwords and password managers cost little; MFA is free or low-cost; updates are free and often automatic; backups require modest investment; training requires time more than money; policies can be adapted from templates; physical security is straightforward and inexpensive. Organizations that implement these practices systematically and consistently become significantly more resilient than those investing in expensive products while neglecting fundamentals.

Security Is a Journey, Not a Destination

Start where you are, progress incrementally using the 30/90/365-day roadmap, measure and celebrate progress through regular self-assessment, learn from incidents rather than assign blame, and adapt to change as your organization and the threat landscape evolve.

The Human Element Is Central

The most sophisticated security technology fails if people don't understand or use it properly. Security-aware people can compensate for limited technology through vigilance and good judgment. This is why the guide emphasizes clear communication, practical practices, no-blame reporting culture, regular training, and shared responsibility.

Balance Security With Usability

Security measures that make work impossible get circumvented. Password managers make strong passwords easier, MFA adds seconds rather than hours, and clear policies reduce uncertainty. When security creates significant friction, work with employees to find solutions that maintain protection while supporting productivity.

You Don't Have to Do This Alone

The Canadian Centre for Cyber Security, the Linux Association of Canada, IT service providers, peer organizations, and industry associations can all help. Don't hesitate to seek assistance for complex challenges.

Your Next Steps

- Complete the Security Self-Assessment to understand your current posture
- Begin the First 30 Days roadmap to start systematic improvement
- Download companion resources from linuxassociation.ca/resources
- Share this guide with colleagues, partners, and peers
- Commit to consistent practice of security habits

Cybersecurity is not about perfection—it's about consistent improvement. Every measure you implement, every employee you train, every policy you establish, and every backup you test makes your organization more resilient.

Protect your people. Protect your information. Protect your community.

About the Linux Association of Canada

The Linux Association of Canada is a national organization dedicated to promoting digital sovereignty, open source technology, and cybersecurity awareness across Canada.

Our Mission

We believe digital sovereignty—the ability of individuals, organizations, and nations to control their own digital infrastructure and data—is essential for privacy, security, and independence. We promote Linux and open source software as foundations for achieving this sovereignty while building secure, resilient, and sustainable digital systems.

What We Do

Education and awareness

Cybersecurity awareness programs, Linux and open source education, school outreach, community workshops, and public awareness campaigns.

Digital sovereignty advocacy

Promoting open source in government and education, supporting Canadian control of digital infrastructure, advocating for privacy protection, and building Canadian capacity in cybersecurity.

Linux and open source promotion

Demonstrating Linux capabilities, supporting organizations migrating to open source, connecting users with communities, and showcasing Canadian contributors.

Community building and cybersecurity support

Connecting individuals and organizations, supporting local Linux user groups, organizing events, and publishing practical guides, templates, checklists, and tools like this one.

Why Linux and Open Source for Security?

Transparency (code reviewable by anyone), community security review, rapid patching, no vendor lock-in, customization, longevity (community-maintained even after vendor discontinuation), and cost-effectiveness that makes robust security accessible to organizations of all sizes.

Our Values

Openness, security, sovereignty, accessibility, community, and sustainability.

Get Involved

Individuals can join community forums, attend workshops, contribute to open source projects, and volunteer for outreach. Organizations can access resources, participate in awareness programs, and support open source adoption. Educators can access school outreach materials and connect with other open-source educators.

Resources and Contact

Visit linuxassociation.ca/resources for cybersecurity guides, policy templates, Linux adoption guides, training materials, and community forums. All companion resources for this guide are available for free download.

Website: linuxassociation.ca • Email: info@linuxassociation.ca

CYBERSECURITY STARTS WITH GOOD HABITS

Protect your people. Protect your information. Protect your community.

Your next steps:

Complete the Security Self-Assessment • Begin the First 30 Days roadmap
Download companion resources • Share this guide • Commit to consistent practice

Linux Association of Canada

Promoting Digital Sovereignty, Open Source Technology, and Cybersecurity Awareness

linuxassociation.ca • info@linuxassociation.ca • linuxassociation.ca/resources

Together, we build a more secure digital future for all Canadians.