



CYBERSECURITY AWARENESS MONTH 2026

A practical guide to recognizing cyber threats, building safer habits, and strengthening business resilience.

FOR BUSINESS LEADERS, IT TEAMS & EMPLOYEES

Awareness is the start. Secure habits make it count.

Explore five common attack methods, lessons from well-known incidents, and the cybersecurity services SWORD provides to help organizations strengthen their defenses.

01 / THE CONTEXT

A month built around everyday action

Cybersecurity Awareness Month turns a technical subject into practical behaviors people can repeat at work and at home.

Launched in **2004**, Cybersecurity Awareness Month began as an initiative of the National Cybersecurity Alliance and the U.S. Department of Homeland Security. It has grown into an international awareness effort involving public agencies, businesses, schools, nonprofits, and individuals. Today, the National Cybersecurity Alliance and CISA continue to lead the campaign in the United States. [1]

2004 | START

A public awareness initiative begins with a simple idea: online safety is part of everyday life.

A WIDER MOVEMENT

As digital services expanded, the campaign grew to address mobile security, identity theft, ransomware, social engineering, and data breaches.

2026 | HABITS

The NCA theme is **"Don't Make It Easy for Them"**: repeat small, reliable actions that reduce opportunities for attackers. [1]

2026 CAMPAIGN MESSAGE

Make life harder for cybercriminals. Strong security is rarely one perfect decision. It is a series of good decisions - checking a message, using MFA, updating a device, and reporting something suspicious.

Four habits worth reinforcing every month

01 Strong passwords

Use a long, unique password for each account and store it in a reputable password manager.

02 Turn on MFA

Add a second factor to email, remote access, cloud tools, and administrator accounts.

03 Recognize & report scams

Pause on urgent or unusual requests. Report suspicious messages using your company process.

04 Update software

Install supported security updates promptly and remove software that is no longer needed.

Why it matters: Cybersecurity is a shared responsibility. Employees make safer decisions, security teams provide guardrails, and leaders fund the people, processes, and technology that make those decisions easier.

02 / CASE STUDIES

When cyber incidents become business incidents

These stories show how gaps in patching, access, and response planning can ripple into essential services.

CASE FILE 01

WannaCry: a warning that moved faster than the patch cycle

On 12 May 2017, WannaCry spread rapidly across vulnerable Windows systems around the world. In England, NHS organizations found systems and devices locked or unavailable, disrupting care and forcing staff to fall back on workarounds. The UK National Audit Office later reported disruption across at least 81 of 236 NHS trusts, as well as hundreds of other healthcare organizations. Thousands of appointments were cancelled, and the incident exposed how unsupported and unpatched systems can become an operational risk - not just an IT problem. [3]

THE LESSON Maintain an accurate asset inventory, retire unsupported systems, prioritize critical patches, segment networks, and rehearse recovery plans before a crisis.

SOURCE [3] UK National Audit Office, [WannaCry and the NHS \(2017\)](#)

CASE FILE 02

Colonial Pipeline: the impact reached beyond the network

In May 2021, a ransomware incident at Colonial Pipeline led the company to proactively shut down its pipeline system while it responded. The FBI confirmed that the DarkSide ransomware was responsible for the compromise. The pipeline restarted several days later. The event showed how a cyber incident affecting a company's digital environment can create broader operational disruption, public concern, and pressure on continuity plans - even when the immediate technical problem starts inside a network. [4][5]

THE LESSON Prepare for service disruption as well as data loss. Keep tested backups, define incident roles, and plan how critical operations can continue safely.

SOURCES [4] FBI statement (2021); [5] U.S. Department of Energy

THE SHARED PATTERN

Small weaknesses can have outsized consequences. The incidents differed, but both underline the value of patching, visibility, tested response plans, clear ownership, and calm, practiced decision-making.

02 / CASE STUDIES

SolarWinds: when trusted software became a route in

A supply-chain incident can bypass the assumption that software from a familiar vendor is automatically safe.

CASE FILE 03

SolarWinds: the update that carried a hidden passenger

In December 2020, U.S. authorities disclosed a far-reaching compromise involving SolarWinds Orion software. Attackers inserted malicious code into the software build process, and the code was distributed through legitimate software updates. For affected organizations, the danger was difficult to spot at first: the initial access path looked like a routine update from a trusted supplier. CISA warned organizations about active exploitation and issued mitigation guidance. Investigations later described a broad campaign that targeted government and private-sector environments. [6][7]

THE LESSON Assess supplier risk, restrict the privileges of management tools, verify unusual authentication and software behavior, and ensure response plans include third-party compromise.

SOURCES [6] CISA alert (2020); [7] MITRE ATT&CK SolarWinds campaign

Trust must be verified

Treat vendor access and software updates as important parts of your attack surface. Review supplier access and security assurances.

Visibility matters

Monitor identity, endpoint, and network activity for unusual behavior - including activity from legitimate administrative tools.

Practice the response

Know who leads the response, who communicates with suppliers, and how affected systems can be isolated and restored.

QUESTIONS TO ASK YOUR ORGANIZATION

- **Assets:** Do we know which systems, devices, applications, and suppliers are critical?
- **Access:** Are privileges limited, reviewed, and monitored - including those used by third parties?
- **Recovery:** Can we restore essential systems from known-good backups and validate that they are clean?
- **Ownership:** Who makes the decisions during a major incident, and have those roles been tested?

KEY TAKEAWAY

Supply-chain security means reviewing trusted software, third-party access, and incident response together - not in isolation.

01

Phishing

A deceptive message tries to make a person reveal information, approve a transaction, open a harmful attachment, or visit a fraudulent page.

A MESSAGE THAT FEELS URGENT

"Your account will be disabled today. Sign in now to avoid losing access." The branding may look familiar and the language may sound professional. The pressure is part of the tactic: attackers want the recipient to act before verifying the request.

Common mistakes

- Clicking first and checking the sender later.
- Trusting a display name or logo without inspecting the actual address or destination.
- Opening unexpected attachments or scanning unknown QR codes.
- Approving MFA prompts that you did not initiate.
- Failing to report a suspicious message because it might be a false alarm.

Warning signs

- Unexpected urgency, secrecy, or threats.
- Requests for credentials, MFA codes, payment, or sensitive data.
- A sender address or link that does not match the claimed organization.
- An unexpected invoice, shared file, delivery notice, or password reset.
- A request to bypass normal approval procedures.

BEST PRACTICES & SOLUTIONS

- Verify unusual requests through a separate trusted channel - especially payment changes, sensitive data requests, and executive instructions.
- Use multifactor authentication, email filtering, and domain authentication controls where appropriate.
- Train staff with realistic simulations and make reporting simple, blame-free, and fast.
- Use the company-approved report-phishing process. If you clicked or entered credentials, tell IT/security immediately; change credentials from a trusted device and follow the incident process.

Remember: a polished message can still be fraudulent. Verify the action, not just the appearance. Guidance: CISA and FTC phishing advice. [8][9]

THE THREE-STEP REFLEX

Pause. Do not use the link. **Verify.** Contact the sender independently or navigate to a known official site. **Report.** Use your approved security channel.

02 Trojan horse malware

A Trojan disguises itself as a legitimate file, app, browser update, or document. Once run, it may steal information, open a backdoor, or install more malware.

HOW A TROJAN TYPICALLY GETS A FOOTHOLD

01 Looks useful

02 User installs / opens

03 Malicious code runs

04 Data or access at risk

Common mistakes

- Downloading cracked software, unofficial installers, or attachments from unknown sources.
- Trusting a fake "security alert" or browser update that appears in a web page.
- Installing browser extensions without checking the publisher and permissions.
- Running files with administrator rights when they do not need them.
- Ignoring unexpected device behavior after a download.

Best practices & solutions

- Download software only from verified vendor sites or approved company portals.
- Keep operating systems, browsers, and endpoint protection updated.
- Use standard user accounts for everyday work; restrict admin rights and application execution.
- Apply web and email filtering, endpoint detection, and application controls where appropriate.

SIGNS THAT DESERVE INVESTIGATION

- New or unfamiliar apps, browser redirects, unusual CPU activity, or security tools unexpectedly disabled.
- Unexpected logins, unknown remote-access tools, or files sent from your account without your knowledge.
- Repeated prompts to install updates from a website instead of the official application updater.

A Trojan is a delivery method, not just one specific kind of malware. It can be used to install other threats, including information stealers and ransomware. [10]

IF YOU SUSPECT A TROJAN

Stop sensitive work on the device and contact IT/security immediately. Follow instructions for isolating it, preserve the suspicious file or message for investigation, and do not try to remove the malware yourself unless authorized.

03 Ransomware

Ransomware can encrypt systems and data, disrupt operations, and be paired with data theft or extortion. The impact may extend to customers and business partners.

OPERATIONS

Files, apps, or services unavailable

CONFIDENTIALITY

Sensitive data may be stolen or threatened

CONTINUITY

Recovery time, cost, and trust are at stake

Common mistakes

- Leaving critical systems unpatched or running unsupported software.
- Keeping backups permanently connected or never testing restoration.
- Giving broad administrative access to everyday accounts.
- Assuming antivirus alone is a complete ransomware defense.
- Delaying escalation because the first symptoms seem minor.

Best practices & solutions

- Maintain offline or otherwise isolated backups and test restores regularly.
- Patch known exploited vulnerabilities and prioritize internet-facing systems.
- Use least privilege, multifactor authentication, endpoint protections, and network segmentation.
- Monitor for unusual logins, mass file changes, and suspicious remote access.
- Practice incident response and business continuity with realistic scenarios.

IF RANSOMWARE IS SUSPECTED

- Activate your incident response process and contact the designated security team immediately.
- Isolate affected devices or network segments according to the response plan; avoid actions that could destroy evidence.
- Preserve logs and key details, protect unaffected backups, and coordinate communications through the incident lead.
- Do not assume paying guarantees recovery or prevents disclosure. Engage qualified responders, legal counsel, and relevant authorities as appropriate.

Ransomware guidance: CISA StopRansomware Guide. [11]

A QUICK REMINDER

Backups matter most when recovery has been tested. Keep recovery copies protected from routine admin access and verify that restoration procedures still work.

04

DNS spoofing

DNS spoofing or tampering manipulates name-resolution information so a domain can lead to an unintended destination. A user may type the correct address and still be redirected if a resolver, router, endpoint, or DNS record has been compromised.

A CORRECT ADDRESS, AN UNEXPECTED DESTINATION

An employee types the company sign-in URL but lands on a convincing imitation page. Nothing looks obviously wrong, so they enter credentials. The risk is not just a suspicious link - it is that name resolution or network settings may be sending traffic somewhere it should not go.

Common mistakes

- Ignoring browser certificate warnings or unexpected redirects.
- Leaving router, registrar, or DNS administration credentials at default values.
- Allowing unapproved DNS resolvers or unauthorized configuration changes.
- Assuming the correct domain typed into a browser guarantees a safe connection.

Best practices & solutions

- Use trusted DNS resolvers and restrict who can change DNS settings.
- Protect registrar and DNS provider accounts with MFA and change controls.
- Deploy DNSSEC where suitable, monitor DNS logs, and consider protective DNS controls.
- Investigate unexpected redirects and verify critical sites from a trusted device and network.

IF DNS TAMPERING IS SUSPECTED

- Stop entering credentials or sensitive information on the unexpected page.
- Notify IT/security, preserve the URL and relevant details, and check the site through a trusted device or network.
- Ask authorized administrators to review resolver settings, DNS records, router configuration, and account activity.

REMEMBER

Unexpected redirects are a signal to stop and verify - not to click through warnings. Use the approved IT/security reporting process.

References: NIST Secure DNS Deployment Guide and Canadian Centre for Cyber Security guidance. [12][13]

05

Malvertising

Malvertising uses malicious or compromised online advertisements to send people to fraudulent pages or deliver malware. A familiar website or professional-looking ad does not guarantee that the destination or download is safe.

THE SPONSORED DOWNLOAD THAT ISN'T WHAT IT SEEMS

Someone searches for a popular utility and clicks the first sponsored result. The page looks professional and offers a free download, but the installer is a fake. One click can lead to credential theft, adware, or a more serious malware infection.

Common mistakes

- Clicking the first sponsored result to download an app or tool.
- Installing a codec, browser update, or security tool prompted by an ad.
- Assuming ads on a legitimate site have all been vetted.
- Allowing downloads or browser extensions without checking the publisher and permissions.

Best practices & solutions

- Type the official vendor URL or use an approved software portal.
- Keep browsers and operating systems updated; restrict extensions and downloads.
- Use protective web filtering and reputable endpoint controls.
- Report suspicious ads and unexpected downloads; involve IT if a file ran.

IF YOU CLICKED OR RAN A SUSPICIOUS DOWNLOAD

- Do not enter credentials or approve unexpected sign-in prompts.
- Contact IT/security promptly and explain what you clicked or downloaded.
- Follow organizational instructions for isolating the device and preserving evidence; do not try to clean an affected work device without authorization.

REMEMBER

Treat surprise software offers with skepticism. Obtain software from verified publishers and approved repositories, not from pop-ups or ad-driven download pages.

References: U.S. FTC guidance on fake software ads and Australian Cyber Security Centre resources. [14][15]

04 / SWORD CYBERSECURITY

Build stronger defenses with a clear view of risk

SWORD positions itself as a cybersecurity solutions partner focused on visibility, proactive protection, vulnerability management, security assessments, and enterprise protection. The service mix can be aligned to your risk profile and business priorities. [2]

Security Assessment

Review the security posture, identify weaknesses, and build a prioritized view of risk.

Governance, Risk & Compliance

Strengthen security governance and risk processes, and support alignment with relevant obligations.

Preparation Testing

Evaluate readiness and test assumptions about how teams and systems respond to security challenges.

Security Training

Help employees recognize phishing and social engineering, follow safer practices, and report suspicious activity.

SAST / DAST Services

Assess application security through static and dynamic testing to uncover issues during development and operation.

Device Management

Improve oversight of business devices and support consistent management as part of a broader security program.

TURN SERVICES INTO A PRACTICAL SECURITY PROGRAM

A stronger security posture is built by connecting assessment, governance, testing, training, and device controls - rather than treating them as isolated tasks.

- Start with critical assets and business risks; prioritize the gaps with the greatest likely impact.
- Give employees a clear path to report suspicious activity and make leadership accountable for action.
- Review progress with meaningful measures: remediation status, MFA coverage, reporting rates, and recovery-test outcomes.

Service names and descriptions are based on SWORD's published Cyber Security page. Confirm the scope and deliverables with SWORD for your environment. [2]

05 / MAKE IT ACTIONABLE

Your October action plan - and what comes next

Use Cybersecurity Awareness Month as a launch point for improvements that continue after October.

WEEK 1

Know the assets

List critical systems, owners, business data, and important suppliers.

WEEK 2

Reduce easy wins

Review MFA, admin rights, patching, browser settings, and exposed services.

WEEK 3

Practice response

Run a short phishing or incident tabletop exercise; confirm escalation contacts.

WEEK 4

Measure & repeat

Review findings, assign owners and due dates, and plan next-quarter refreshers.

IF YOU SUSPECT AN INCIDENT

Report it quickly. Contact your internal security/IT lead, follow the incident-response plan, preserve relevant messages and logs, and avoid experimenting on affected devices. Isolate systems only in line with your organization's response instructions. If credentials may be exposed, use a trusted device and follow the approved reset process.

FORTIFY YOUR BUSINESS WITH SWORD

Make cybersecurity a business-strengthening decision.

SWORD combines strategic thinking and cybersecurity expertise through security assessments, GRC, preparation testing, security training, SAST/DAST, and device management. Discuss your priorities with our team.

EXPLORE SWORD SERVICES

www.swordnow.com/cyber-security

SOURCES & FURTHER READING

- [1] National Cybersecurity Alliance, [Cybersecurity Awareness Month 2026](#).
- [2] SWORD, [Cyber Security services](#).
- [3] UK National Audit Office, [Investigation: WannaCry cyber attack and the NHS](#) (2017).
- [4] FBI, [Colonial Pipeline ransomware statement](#) (2021).
- [5] U.S. Department of Energy, [Colonial Pipeline Cyber Incident](#).

- [6] CISA, [Active Exploitation of SolarWinds Software](#) (2020).
- [7] MITRE ATT&CK, [SolarWinds Compromise](#).
- [8] CISA, [Phishing: Simple Tips](#).
- [9] FTC, [Protect yourself from phishing scams](#).
- [10] Australian Cyber Security Centre, [Learn about malware](#).
- [11] CISA, [StopRansomware Guide](#).
- [12] NIST, [Secure DNS Deployment Guide](#) (2026).
- [13] Canadian Centre for Cyber Security, [DNS tampering](#).
- [14] FTC, [Ads for fake AI and other software spread malicious software](#).
- [15] Australian Cyber Security Centre, [Information-stealer malware advisory](#).