Cybersecurity Business Training

A Guide to Preventing Business Cybercrime

Managed IT | Co-Managed IT | Cybersecurity

ANDERSON TECHNOLOGIES

Cybersecurity Business Training Ebook by Anderson Technologies, a St. Louis IT Company
info@andersontech.com | andersontech.com | 314.394.3001 | © 2026 Anderson Technologies

Cybercrime Is Evolving

Cybercrime remains the fastest-growing threat to businesses and individuals in the United States, but it's no longer just growing—it's transforming. Artificial intelligence (AI) is supercharging attackers' capabilities by enabling more convincing phishing lures, AI-generated fraud, and faster, more targeted attacks. As Eva Velasquez, CEO of the Identity Theft Resource Center (ITRC), warns, "The power of AI in the hands of professional criminals is accelerating a shift we've long warned about—where traditional crime patterns give way to a landscape in which anyone can be a victim."[1]

Most cybercrime is preventable, but even if you do everything right, all it takes is one wrong click to breach your digital "fortress." According to the World Economic Forum's Global Cybersecurity Outlook 2026, 94% of cybersecurity leaders say AI is the most significant driver of change in cybersecurity, and 87% identified AI-related vulnerabilities as the fastest-growing cyber risk.[2] That's why it's so important that your entire workforce understands digital best practices and how to protect themselves (and your business) from cybercrime. The U.S. saw a record 3,322 data compromises in 2025, a massive 79% jump over five years.[3]

In this handbook, you will learn about:

- **The state of small business cybercrime**
- **How the threat landscape is changing**
- **Email red flags, including examples of real spear phishing emails**
- **Internet safety tips and warning signs**
- **What to do if you've clicked or downloaded something you shouldn't have**

ANDERSON TECHNOLOGIES

Cyber Threats Against Mid-Sized Businesses Are Growing

Over the last few years, cybercriminals have increasingly set their sights on mid-sized businesses. According to Verizon's 2025 Data Breach Investigations Report, SMBs are being targeted nearly four times more than large organizations.[4] Sophos' State of Ransomware 2025 report found that businesses with 100–250 employees faced an average recovery cost of $638,536 per attack—and that's before any ransom payment is factored in.[5]

"There is no such thing as a business so small it can fly under the radar of the threat actors." – Verizon, 2025 Data Breach Investigations Report[4]

Part of the reason mid-market businesses are increasingly targeted is because many do not take the necessary steps to stay secure. This makes them easy targets.

To ensure digital safety, every business must:

1. Implement a continuously monitored and updated firewall, or deploy a Zero Trust Network Access (ZTNA) system to secure your network.
2. Install antivirus and anti-malware software on all devices and keep them updated.
3. Back up all business-critical files regularly and test their ability to be restored.
4. Regularly update all your devices' operating systems and third-party security patches.
5. Adopt a zero-trust approach. Share data only with those who need it, and continually evaluate every access request.
6. Educate employees about cybersecurity best practices regularly, including how to recognize AI-powered phishing and social engineering tactics.

The last point is crucial. Even with steps one through five in place, a single wrong decision by an employee can undo all your efforts, so systems must be ready for when that happens.

Cybercriminals Are More Sophisticated

Phishing emails are a cybercrime tactic in which the sender attempts to steal personal information, passwords, or session tokens to impersonate the recipient or access their account. They are sent to a wide audience, and many people have learned to spot the telltale signs: awkward phrasing, strange spelling errors, or requests that seem too good to be true.

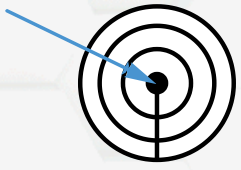
But those obvious red flags are becoming a rarity. Today's phishing emails are more polished and harder to detect, in part because attackers are using tools like generative AI to produce convincing, error-free messages at scale. Phishing has also evolved into spear phishing, a more sophisticated con in which a criminal targets a specific person and crafts a believable email based on personal information obtained about the recipient.

Spear phishing emails often appear to come from a colleague, friend, family member, or business associate, usually arriving in your inbox well designed and written convincingly enough to seem legitimate.

How Hackers Access Personal Information

Even if you've done everything right, cybercriminals could still glean enough information to target you via a phishing scam. For example, they may have hacked a site with your contact information, such as an online shopping company or an email provider. Your data can even be compromised by companies you have never interacted with. In April 2024, data broker National Public Data suffered a massive breach that exposed up to **2.9 billion personal records**—including names, Social Security numbers, and home addresses—belonging to individuals who had likely never heard of the company.[6] This is the type of incident that gives cybercriminals the information they need for more convincing scams.

Phishing: Emails are sent to a wide audience in the hopes someone will fall for the scam.

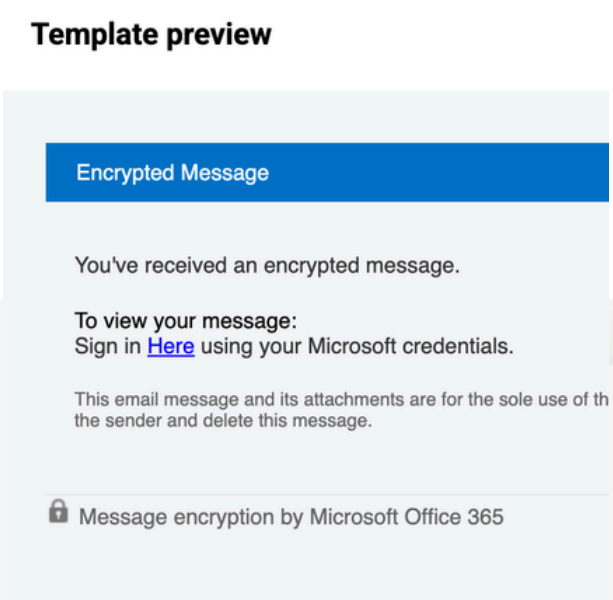


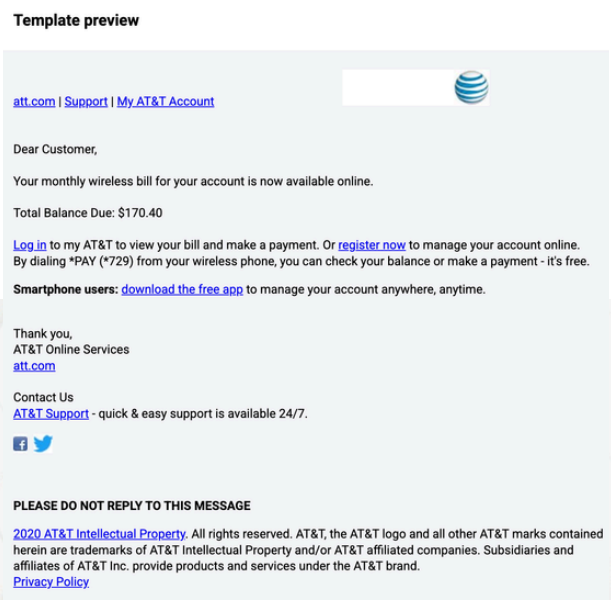
Spear Phishing: Emails are personalized and designed to trick a particular target. They are harder to recognize as fraudulent.

Your Email Best Practice Checklist

The screenshots below show examples of spear phishing emails. As you can see, they look quite convincing. Fortunately, simply opening an email is unlikely to do any harm on its own. It's clicking a link or downloading an attachment that allows the criminal to infiltrate your system.

Examples of Spear Phishing Emails

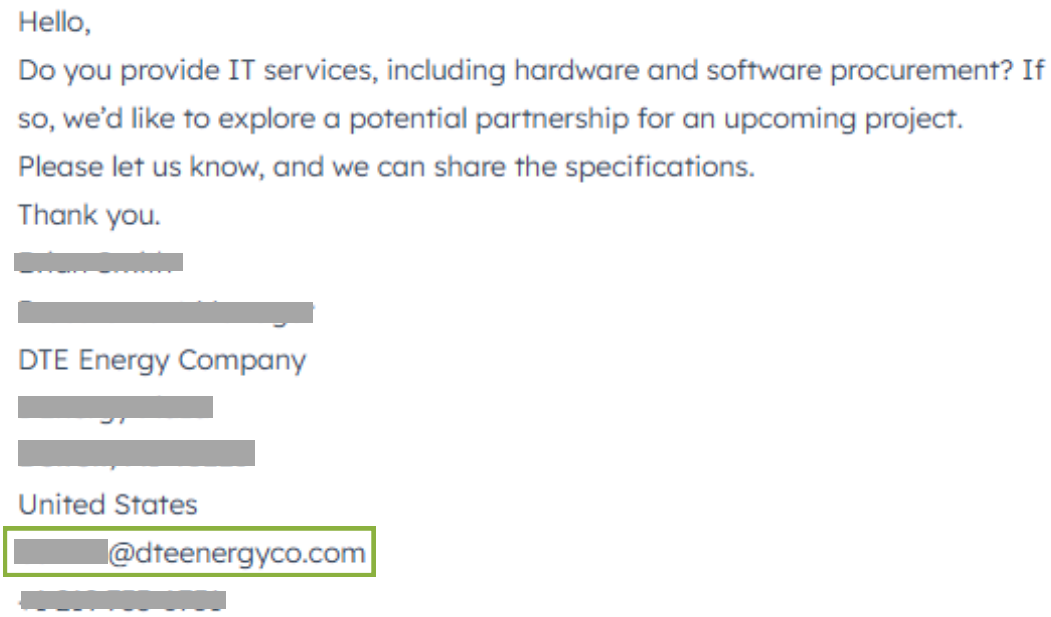




Your Email Best Practice Checklist

Although phishing emails can be convincing, there are ways to identify them as fraudulent before you give them your information or click a dangerous link.

Example


Hello,
Do you provide IT services, including hardware and software procurement? If so, we'd like to explore a potential partnership for an upcoming project.
Please let us know, and we can share the specifications.
Thank you.
[redacted]
[redacted]
DTE Energy Company
[redacted]
[redacted]
United States
[redacted]@dteenergyco.com
[redacted]

Incorrect Email Address

Examine the email address. Notice in this example, the email address uses "@dteenergyco.com" instead of "@dteenergy.com."

Suspicious URL

If the email contains a link, hover your mouse over it before clicking. While it might look legitimate in the body of the email, it might not be as real as it seems upon first inspection.

Your Email Best Practice Checklist

1 Are they asking me for private or personal information?

Consider the nature of what the sender is asking for. Financial organizations will **NEVER** ask you to provide personal information like account numbers or passwords via email. Email is not secure, so a legitimate bank will only ask for private information via a secure site after you have already proven your identity, ideally through a multi-factor authentication process (in which you take two or more steps to prove that you are who you say you are, such as entering a password and then confirming via an authenticator app or a code sent to your phone). Be alert if a sender is asking for personal information directly.

2 Does it seem too good to be true or just slightly off?

Phishing emails don't always promise something outlandish. While some are still recognizable because they offer deals that seem too good to be true, many modern phishing attempts are more subtle. They may mimic routine messages you'd normally act on without thinking: a password reset, a shipping notification, or an invoice from a familiar vendor. Always be on high alert, remain skeptical, and take an extra moment to verify before clicking.

3 Where does this link lead?

Before clicking a link, hover over it with your mouse to see the URL. This can be a tip-off. If the URL does not match the sender's supposed company, be wary. Also be wary of URLs that end in domain names from foreign countries. They look like links to genuine sites, but actually direct to websites in the countries where the attackers are based.

4 What is the email address of the sender?

Check the actual email address of the sender, not just the name that shows up in your inbox preview. Even if the email appears to come from a known contact, confirm the address, especially if the emails was unexpected. Be cautious of addresses that seem off, like a Yahoo address claiming to be from a business, or any spelling errors such as in "no-reply@poypol.com."

5 Are there attachments?

Attachments are a huge red flag! By downloading an attachment, you could infect your computer or even your entire business network with malware or viruses. Do not download an attachment unless you are certain of the sender's identity and the content seems legitimate. If you weren't expecting to receive an attachment from the sender, even if you recognize the person, reach out by phone or other non-email channel to confirm it isn't malicious. If you do download an attachment, save and scan it with antivirus software before opening it.

Domains Often Used in Phishing Attacks

Cybercriminals often register phishing sites using inexpensive domain extensions. Security research from Spamhaus and Interisle shows domains such as **.xyz**, **.top**, **.online**, and **.site** frequently appear in phishing campaigns. This doesn't means every site using those domains is malicious, but it's wise to **double-check unfamiliar links before clicking.**

The Rules for Safe Surfing

Everyone needs to be mindful of web-browsing best practices. With one wrong click, you could infect your computer with dangerous malware that allows a criminal to affect your computer's performance or obtain personal information about you, your business, or customers. You cannot passively surf the web. Be alert, think before you click, and try not to visit sites you've never heard of. Here's what you need to know.

1 Risky content means risky sites

Cybercrime is rampant on sites where people are doing something they probably shouldn't. Pornography and any illegal activity are prime targets for cybercriminals, in part because the sites' administrators probably aren't taking the steps necessary to protect their visitors. Stay off these types of sites, especially at work or when you are remotely connected to your work network.

2 Dangerous sites can show up in searches

Even innocuous behavior can land you in dangerous territory. Criminals create sites cleverly designed to trick users into believing they are legitimate. Plus, real sites can get hacked. Let's say you are searching for a gift on your lunch break and end up on a small e-retailer you've never heard of, a site that happens to have been hacked. A criminal could access your password and credit card information when you enter it on the affected site!

3 Use the "safe search" feature

Antivirus and anti-malware programs often offer a "safe search" feature that runs search results through their own database to rate the safety of sites and flag any URL they know to be compromised. If your business takes this security precaution, do not visit sites deemed unsafe by your antivirus provider.

4 Install a firewall for enhanced protection

A firewall acts a virtual barrier between your network and the outside world, preventing unauthorized access through open ports or protocols. An enterprise-grade hardware firewall offers additional features to filter specific types of content and provide extra layers of malware protection, or you can implement a Zero Trust Network Access (ZTNA) system for more granular access control. If you don't have a hardware firewall, a managed services provider can help you set one up and provide the necessary ongoing maintenance of firewall settings. But remember, firewalls can't block everything, such as zero-day threats, which are new attack vectors written to take advantage of previously undocumented flaws in a piece of software. Always stay alert and follow cybersecurity best practices.

The Rules for Safe Surfing

5 Be careful when downloading things from the web

Cybercriminals do their damage by getting you to click a web link or download a nefarious attachment. The absolute safest approach would be to never download anything from the web, but we know in today's business environment that is not realistic. Proceed with caution, always scan files before downloading them, and if you are unsure if something is safe, run it by your IT partner or your manager first.

6 Exercise caution when working remotely

Remote and hybrid work is now the norm for many businesses, but it comes with real cybersecurity risks. Whenever you use a company asset—such as a laptop, tablet, or smartphone—think before you connect to any Wi-Fi network. Even your at-home connection could be dangerous! If your home environment is not fully protected with up-to-date operating system patches, antivirus definitions, firewall firmware, etc., it could be laced with problems. If you connect your company laptop, you could infect it and bring the malware back to your workplace.

7 Limit or eliminate browser extensions

Data leakage is a serious problem, especially when workers use their personal computers to access company data remotely. Browser extensions, even legitimate ones, can siphon data without the user realizing it. Avoid all unnecessary browser extensions to limit the risk to company or client data.

How to Tell If an Online Retailer Is Legitimate

1 Check that the URL starts with HTTPS instead of HTTP. "S" stands for "secure" and means the site encrypts the traffic passing between it and your browser.

2 Make sure the site name looks legitimate, doesn't have strange spelling errors, and isn't trying to imitate a well-known site.

3 Confirm that the business the site represents has a physical address and phone number.

4 Check for a privacy policy, return policy, and other signs that the site is legitimate, such as a social media presence and user reviews.

5 Use common sense! If something seems too good to be true (i.e., the prices are incredibly low), be skeptical and leave the site.

ANDERSON TECHNOLOGIES

The Art of Password Management

According to the latest edition of NordPass' Top 200 Most Common Passwords, **"123456"** remains the most common password in the world for the sixth year out of seven—followed by familiar offenders like "admin" and "password."[7] Even more alarming, 78% of the world's most common passwords can be cracked in less than a second.[8] Take the following steps to improve password security.

Use a password management tool to help you create and keep track of secure passwords.

If you ever fear your cybersecurity has been compromised, change your passwords immediately.

Use a breach monitoring service, and change any passwords that have been leaked, along with any accounts connected to the compromised one.

Create passwords with random words you can easily remember. Avoid obvious things like names of loved ones or birthdates. Current guidelines recommend combining 4–5 unrelated words to create a long, strong password you can remember easily.

Use a minimum of twelve characters. The longer the password, the stronger it is. A mix of uppercase and lowercase letters, numbers, and special characters make it even harder to crack.

Enable multi-factor authentication (MFA) wherever possible. Even the strongest password can be stolen. MFA adds an extra layer of protection by requiring a second step, like a code from an authenticator app or a text to your phone, before granting access.

Artificial Intelligence and Cybersecurity

Artificial intelligence (AI) is rapidly transforming the cybersecurity landscape. While businesses use AI tools to strengthen defenses and automate security monitoring, cybercriminals are also using AI to make their attacks faster and harder to detect.

AI can analyze large amounts of data quickly, allowing attackers to automate phishing campaigns and identify system vulnerabilities at scale. Organizations must stay aware of how AI is influencing both cyber threats and cybersecurity protections.

AI-Powered Cyber Threats

AI is increasingly being used to automate cybercrime. According to the 2026 CrowdStrike Global Threat Report, there has been an 89% increase in attacks by AI-enabled adversaries. As these tools become easier to access, cybercriminals can launch larger and more sophisticated attacks with less effort.

How to Protect Your Business

AI-powered threats make strong cybersecurity habits more important than ever.

- **Be cautious with emails and messages.** AI-generated phishing attempts can closely mimic trusted contacts or legitimate companies. Always verify unexpected requests for information, payments, or login credentials before responding or clicking links.
- **Keep security software updated.** Up-to-date antivirus and anti-malware tools help detect new and evolving threats. Enable automatic updates whenever possible so your systems receive the latest protections without delay.
- **Train employees regularly.** Awareness training helps staff recognize suspicious messages and social engineering attempts. Regular training also helps employees stay informed about new tactics cybercriminals use as technology evolves.

AI-Powered Deception: Deepfakes and Voice Cloning

Cybercriminals aren't just getting smarter; they're using smarter tools. Today's attackers can use AI to clone a person's voice from just a few seconds of audio and generate realistic video of someone who isn't there. According to CrowdStrike, AI-based voice cloning attacks surged 442% in the second half of 2024 alone.[10]

And it's not just executives being targeted—criminals use the same technology to impersonate coworkers, IT support, vendors, and even family members. A McAfee study found that 1 in 4 adults have already encountered an AI voice scam.[11]

The $25 Million Video Call

In early 2024, a finance worker at global engineering firm Arup received an email from someone claiming to be the company's UK-based CFO about a confidential transaction. The employee was initially suspicious but then joined a video call with the CFO and several senior colleagues to discuss the details.

Every face on the screen looked real, and every voice sounded right, but every person on that call (except the victim) was an AI-generated deepfake.

The result: $25 million transferred to fraudsters before anyone realized what had happened.[12]

As Arup's Global CIO later described it, the attack was "technology-enhanced social engineering." The attackers didn't breach firewalls; they breached human trust, amplified by AI.

How to Protect Yourself

The uncomfortable truth is that deepfakes are now good enough that most people can't reliably detect them. The best defense is not trying to spot every fake but building habits that verify requests through trusted processes.

Verify requests through a separate channel. If someone asks for a payment, password, or sensitive information, confirm the request using a known phone number or internal contact instead of replying to the email or message directly.

Avoid clicking links in unexpected emails. Instead of following a link in a message, navigate to the company's website manually or use a saved bookmark to access your account.

Question urgency and pressure. Social engineering attacks often push victims to act quickly before they can verify the request through proper channels.

Use internal approval controls for financial requests. Businesses should require multiple approvals for large payments or wire transfers so a single employee cannot authorize a fraudulent transaction.

What to Do When You Think Your Cybersecurity Is Compromised

Following digital best practices will help you avoid cyber threats, but the bad guys are so sneaky that they can trip up even the most cautious among us. Mistakes happen.

Sometimes a virus will go completely unnoticed. Other times, it may affect computer performance, especially if you have an older machine.

If you click a link and are unsure about where it leads or what appears, download an attachments and feel uneasy about what happens next, or simply feel uncomfortable for any reason, trust your instincts and take the following steps.

1. Call your IT partner any time you need assistance., and their advice for your specific situation should override the following if necessary.
2. Don't click anything, not even an "X" to close a pop-up box.
3. Disconnect from the network by either physically removing the network cable if your machine is hardwired or by turning off your computer's Wi-Fi connection.
4. Reboot your computer in Safe Mode and run a full system scan with your antivirus and anti-malware software.
5. If an unresolved issue is identified, ensure you have an existing backup of your data, reformat your hard drive, reinstall the operating system, reinstall all third-party software, and restore your data from the known good backup. Your IT provider can walk you through this process or handle it for you.
6. Perform a second system scan to ensure your machine is clean.
7. Reset all critical passwords. Monitor your sensitive data and financial accounts.

If you didn't actually click the harmful link or download anything dangerous, a simple reboot may be all you need. If everything appears fine, ensure your antivirus and anti-malware software is up to date and run a full system scan. Clear your browser cache (a good step to take routinely) and change your passwords for extra security.

"X" Does Not Mark the Spot

If you are suspicious of a pop-up, don't try to close the window by clicking the "X"! Even though you are trying to dismiss the threat, the simple act of clicking could be enough to infect your computer. Instead, disconnect from your business network and call an IT expert right away.

Bottom Line? Be Skeptical.

Be skeptical about every email you receive, every website you visit, and every unexpected call or video chat that asks you to take action. Do not move passively through the digital realm. Liken it to a bustling market with a notoriously high rate of theft. You wouldn't go around giving personal information to every random person who asked—and you wouldn't wire money just because someone who looked familiar told you to. Stay alert, verify before you act, and think before you click.

Endnotes

1. Eva Velasquez, CEO of the Identity Theft Resource Center, **as quoted in Infosecurity Magazine, June 2025.**
2. World Economic Forum, **Global Cybersecurity Outlook 2026** (January 2026).
3. Identity Theft Resource Center, **2025 Data Breach Report** (January 2026).
4. Verizon, **2025 Data Breach Investigations Report** (May 2025).
5. Sophos, **The State of Ransomware 2025** (June 2025).
6. IBM, "**2024 Roundup: Top Data Breach Stories and Industry Trends**" (December 2024).
7. NordPass, **Top 200 Most Common Passwords** – 7th Edition (November 2025).
8. NordPass, **Top 200 Most Common Passwords** – 6th Edition (November 2024).
9. CrowdStrike, **2026 Global Threat Report** (February 2026).
10. CrowdStrike, "**2025 Global Threat Report: Beware the Enterprising Adversary**" (February 2025).
11. McAfee, "The Artificial Imposter" study (2024), as cited in DeepStrike, "**Deepfake Statistics 2025.**"
12. Multiple sources, including **CNN** and the Financial Times, widely reported February–May 2024.

About Anderson Technologies

We hope you found this ebook useful. Educating yourself and your team is an integral and often overlooked component of cybersecurity.

Don't miss out on the peace of mind that comes with employees trained to recognize today's cyber threats, from phishing and social engineering to AI-powered scams. Contact Anderson Technologies' team of experts to schedule a free cybersecurity training session for your employees, and know that your business is one step closer to preventing a cyberattack.

Click to Schedule a Free Consultation

Click to View All Our Free Resources

Have Any Questions?

The team at Anderson Technologies is happy to discuss any questions you have or schedule a time to help educate your employees about best practices. Give us a call today at 314.394.3001.

Managed IT | Co-Managed IT | Cybersecurity