Reducing Employee IT Liability

An Employer's Guide

Managed IT | Co-Managed IT | Cybersecurity

ANDERSON TECHNOLOGIES

Reducing Employee IT Liability

We discussed in-depth the importance of employee training in reducing your business's IT liability in this **blog post.**

We'll cover the most **important aspects** of IT to educate your team on, the biggest cyber threats they're likely to face, and provide **examples of good** (and bad) cybersecurity practices in action. Use this guide with expert-led cyber safety **training sessions** to refresh your and your staff's knowledge.

Why Worry and Common Cyber Threats

Your employees are your greatest asset, but they can also become a significant liability if they aren't made aware of the IT dangers they face at work. Reputational damage from a cyber incident can be catastrophic, leading to loss of customer trust, legal consequences, and financial losses. Ensuring your team is well-informed and vigilant can help prevent such outcomes.

Don't make the mistake of thinking cybersecurity is a concern reserved for your IT team—business-wide awareness is a must.

ANDERSON TECHNOLOGIES

Educate Your Team

Common Cyber Threats

Let's outline some of the digital dangers the average worker will encounter day-to-day.

Social Engineering: An umbrella term for the techniques cybercriminals use to manipulate people into divulging confidential information or performing actions that compromise security. Most of the threats your team faces will involve some form of social engineering. These predominantly occur via email, which is many businesses' primary form of communication.

Key threats include:

- **Phishing:** Tricking individuals into providing sensitive information, like passwords or credit card numbers, by pretending to be a trustworthy entity, often through a deceptive email or website.
- **Malware:** Malware, or malicious software, includes viruses, ransomware, and spyware that can infect and damage computer systems, steal data, or block access to files until a ransom is paid.
- **Business Email Compromise (BEC):** A type of scam where attackers impersonate a company executive or trusted business partner to trick employees into transferring money or sharing sensitive information.

Vigilance and Endpoint Protection

It might get tiresome to hear about the same dangers time and time again, but vigilance here should be prioritized.

Employees can inadvertently cause significant harm if they fall victim to these threats, so continuous education and awareness are crucial.

Look Out For:

1. Unexpected emails from unknown senders.

2. Suspicious links or attachments hover over links before clicking on them; if the URL doesn't match what you'd expect based on the text in the email, don't click.

3. Requests for urgent actions or sensitive information. Even if it appears to be from someone within the organization, it's best to verify these with the supposed sender on another platform before handing over any details.

Educate Your Team On Endpoint Protection

In today's interconnected environment, it’s not uncommon for employees to use multiple devices, including laptops, smartphones, and tablets, at work. Each device presents a potential entry point for cyber threats.

It’s important to keep them all protected through:

Use of Antivirus Software: Ensure all devices have updated antivirus software. This will help detect and removes malware, providing real-time protection and keeping systems secure.

Regular Updates: Keep operating systems and applications up to date to patch vulnerabilities. This also improves functionality, reducing lag and crashes.

Device Encryption: Encrypt sensitive data on all devices. Even if the data is intercepted or devices are lost, the information remains unreadable to unauthorized users.

Secure Access: Implement strong passwords and multi-factor authentication (MFA). This ensures only authorized personnel can access sensitive information and systems.

Your team should know why each of these steps is important to follow on all their devices—especially if your business has a BYOD (Bring Your Own Device) policy.

People are more careless with their personal devices, and the consequences of lax security need to be made clear.

ANDERSON
TECHNOLOGIES

Educate Your Team On the Importance of Reporting

To ensure swift and effective responses to potential security threats, it is crucial that all employees are well-informed on the proper procedures for reporting suspicious activities.

Employees should know how and to whom to report suspicious activities.

Establish clear protocols for:

1. Who to Report To: Designate a specific person or team responsible for handling IT security issues.

2. What to Report: Encourage reporting of phishing attempts, suspicious emails, and any other unusual activity. Also, any lost equipment or accidental disclosure of confidential information.

3. When to Report: Remind employees to inform someone even if they've already clicked on something suspect. It might not be too late to prevent the damage spreading to other devices or users.

4. How to Report: Provide easy-to-use reporting channels, such as email, phone, or an IT helpdesk.

Practical Protective Measures

Best Practices in Daily Workflows

To reduce IT liability, integrate the following best practices into your team's daily routines:

1. Email Vigilance

- Avoid engaging with emails from unknown senders.
- Be cautious of odd subjects or links in emails.
- Verify the authenticity of requests for sensitive information.

2. Online Presence

- Be cautious about what’s posted online. A computer screen in the background of a photo or video could accidentally expose sensitive information, so always double check before hitting ‘share’. Better yet, don’t post anything from your workplace to either a personal or business account.

3. Secure Wi-Fi Usage

- Only use secure, password-protected Wi-Fi networks.
- When working from public places like cafes, employ a Virtual Private Network (VPN).

4. Strong Passwords and MFA

- Use complex passwords that include a mix of letters, numbers, and symbols.
- Change passwords regularly.
- Enable multi-factor authentication (MFA) for an added layer of security.

5. Software Updates

- Regularly update all software to protect against vulnerabilities. Even the minor patches matter.
- Don’t ignore software update notifications. Schedule them to occur automatically out of working hours to avoid disruption.

6. Physical Security

- Never leave confidential information laying around your workspace. Insider threats are real and dangerous, and a missing Post-It could be hard to spot until it’s too late.

ANDERSON TECHNOLOGIES

Get Realistic: Adopting a "Not If, But When" Mindset

At some point, your team will be targeted by cybersecurity threats. Aim to move away from the avoidant, "don't speak about it, lest you jinx it" approach.

Addressing the elephant in the room with a "not if, but when" mindset helps in preparing and responding effectively:

Building a Resilient Cybersecurity Culture

Incident Response: Foster a culture focused on vigilance rather than blame. Who's responsible for an incident doesn't matter nearly as much as its impact (and learning how to stop it occurring again). Emphasize the importance of the response and learning from incidents over pointing fingers.

Phishing Simulations: Conducting simulations helps reinforce all your training and protocols and see if they've really sunk in. Practical application doesn't have to be reserved for the real thing; treat these as rehearsals that allow you to pinpoint any areas where additional training or reminders are needed. Then, when (not 'if') the real thing comes, your employees will remain cool, calm, and collected, handling cyber threats with confidence.

Cybersecurity Practices in Action

It might be helpful to have some examples to illustrate what an employee using these practices might look like, so your team know what to avoid and what to aim for. Feel free to tailor the following scenarios to suit your business.

Scenario 1: Jane

Jane works in the customer service department of her company. She's working remotely today, enjoying her morning coffee at a nearby café. With her laptop connected to the café's Wi-Fi, Jane begins her workday by opening her email, where she notices a message from an unknown sender with the subject line "URGENT: Invoice Attached." Without thinking twice, she clicks on the attachment and opens it. The document appears blank, but Jane dismisses it and moves on to her other tasks.

By the end of the day, Jane's computer starts behaving strangely. She calls IT support, who informs her that her computer has been infected with malware from the suspicious email attachment. Additionally, her data might have been compromised due to the unsecured public Wi-Fi connection. Jane's negligence and lack of awareness have led to a serious security breach.

Questions For Your Team:

1.) Identify Risks: What are the potential dangers of connecting to public Wi-Fi? What about opening email attachments from unknown senders?

2.) Awareness and Training: How could Jane's awareness of phishing tactics be improved? What training could help prevent this situation in the future?

3.) Preventative Measures: What steps could Jane have taken before opening the attachment to verify its authenticity? What tools or practices can help mitigate risks when working remotely?

Cybersecurity Practices in Action

Scenario 2: John

John is a project manager. Thanks to his annual training, he's aware of basic cybersecurity practices (even if he sometimes overlooks them in favor of convenience). One morning, he receives an email from a familiar-looking source—it's his IT department asking for his login details. The request has something to do with reconfiguring his permissions, which is beyond anything tech-averse John understands. The email looks somewhat suspicious, but hey, the IT guys know what they're talking about. John decides to reply, thinking it's probably safe.

Later, John's working on a project from his office. He uses strong passwords to login to the software he needs. Sure, he uses the same password for multiple accounts on occasion, but he changes it regularly! As he works, he receives another email, this time from a client. The email contains a link to an important financial document. John carefully checks the sender's email address—no spelling mistakes, a familiar, reputable domain—and feels it's legitimate. This particular client is a stickler for promptness, so, not wanting to bother them with a quick verification call, John clicks the link. Fortunately, it turns out to be safe—this time.

In the afternoon, John attends a video conference. Just before joining, he checks his surroundings and screen sharing options, deciding to angle his laptop a little more to the left to avoid the highly sensitive client plan written on the whiteboard behind him appearing in the background.

John's mixed approach to cybersecurity shows some good practices, but he needs to be more consistent and cautious, especially with email security.

Questions For Your Team:

1. Good Practices: What cybersecurity measures is John practicing well, and why are these important?

2. Risk Assessment: Why is it risky to reuse passwords across multiple accounts, and what are the potential consequences?

3. Improvement Steps: How can John verify suspicious emails more effectively? What steps should he take before clicking on links or sharing personal information?

Cybersecurity Practices in Action

Scenario 3: Emma

Emma works in the finance department and is well-trained in cybersecurity practices. She begins her day just like Jane and John—by checking her email. She notices a message from a known sender with the subject "URGENT: Action Required. Verify Your Account Details to Avoid Losing Acces". That's weird, thinks Emma, I haven't requested a password reset, or created a new account anywhere recently. Emma knows it's better to be safe than sorry, so instead of opening it, she forwards the email to the IT department for verification. Best-case scenario, they'll say it's all fine and she'll maybe feel a little silly for a moment before relief takes over at having made the smart call. But IT confirms it is actually a phishing attempt, and Emma deletes it immediately.

Later in the day, Emma receives a USB drive from a trusted client with important files. The company's policy is not to use these for work purposes—all their materials should be stored on their cloud system. Emma trusts this client—they're a friend of the family who cat-sat for her sister last month—but she heeds the warning given out in her cyber training sessions: you can never be too careful. She gives the drive back to the client, and reminds them that any business-related documents need to be delivered to the company as per the proper procedures.

Throughout the day, Emma remains vigilant. She uses strong, unique passwords and multi-factor authentication for all her accounts. She's cautious about what she shares online and never leaves her laptop unlocked while unattended. Emma's consistent use of her cybersecurity training helps her effectively mitigate risks and protect her company's data.

Questions For Your Team:

1. Best Practices: What specific actions did Emma take that demonstrate good cybersecurity hygiene? How do these actions help protect her company's data?

2. Potential Risks: Even with good practices, what areas could still pose risks for Emma? Are there any additional precautions she should consider?

3. Continuous Improvement: How can Emma continue to stay vigilant and up to date with cybersecurity threats? What resources or ongoing training might be beneficial for her?

Empowering Your Team to Mitigate IT Risks

Remember, **cybersecurity is a collective effort.** With the knowledge gained from this guide, your employees can navigate their digital environments more confidently, making **informed decisions** that protect your **business's valuable data** and maintain its integrity. Together, you can build a resilient IT environment that not only mitigates risks, but also fosters trust and security within your **organization.**

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