

TECH BYTES

October 2025

STRENGTHEN SECURITY.
GROW YOUR BUSINESS.



Stay ahead with smarter cybersecurity. Leverage modern tools, make informed choices, and lead confidently in a fast-changing threat landscape.

Matthew DeWees
-President

Your client list and brand reputation are among your most valuable assets but without strong login security, they're at risk. Cybercriminals no longer need to "hack" their way in. Stolen credentials are sold online for less than the cost of lunch, giving attackers easy access to your systems. With the average data breach costing \$4.4 million, the consequences are too big to ignore.

Unfortunately, many employees still underestimate the importance of basic security practices. That's why real protection requires more than just telling people to "use better passwords." Effective login security is built in layers, strong password policies, multi-factor authentication, and a culture of security awareness all play a vital role.

The good news? Securing your business logins doesn't have to be complicated. Small, consistent improvements can create a powerful defense.

✉ Get a free consultation and a custom security plan:
everythingit@virtualdataworks.com
Until then, stay safe.



President



WHAT'S INSIDE?

02 CYBERSECURITY AWARENESS
TRAINING FOR EMPLOYEES

03 ADVANCED STRATEGIES TO
LOCK DOWN YOUR BUSINESS
LOGINS

04 A HACKER'S KRYPTONITE IS MFA

05 TOP 10 CYBERSECURITY POLICIES
EVERY COMPANY SHOULD HAVE

06 THE ADVANCED GUIDE TO
PROTECTING YOUR SMALL
BUSINESS

07 CONTACT AN EXPERT

DID YOU KNOW?

The first computer bug was an actual moth that got stuck in a relay in 1947, leading to the term "debugging"

Virtual DataWorks

📍 475 Wolf Ledges Parkway
Akron, Ohio 44311

🌐 virtualdataworks.com

📞 (330) 800-2186

Cybersecurity Awareness Training for Employees

As digital transformation accelerates innovation, cybersecurity has become a key pillar of organizational resilience. While technology plays a major role in defense, the human factor remains one of the most vulnerable aspects of any security strategy.

That's why employee cybersecurity awareness training isn't just a best practice, it's a strategic necessity.

THE HUMAN FACTOR IN CYBERSECURITY

Despite advanced security tools, human error remains a top cause of cyber incidents. Phishing alone drives over 90% of breaches, often triggered by weak passwords or careless clicks.

Cybersecurity training helps employees spot threats, respond wisely, and build safer habits, making them a key line of defense.



Core Elements of a Robust Training Program

An effective cybersecurity awareness program should be comprehensive, engaging, and tailored to the unique needs of the organization. Key components include:

1. Phishing and Social Engineering Defense

Employees must learn to identify suspicious emails, deceptive links, and fraudulent requests. Training should include real-world examples and simulated phishing exercises to reinforce learning.

2. Password Management and Authentication

Strong password practices and the use of multi-factor authentication (MFA) are essential. Training should cover password creation, storage, and the risks of password reuse.

3. Secure Use of Devices and Networks

Guidelines for using company devices, accessing corporate networks remotely, and avoiding public Wi-Fi for sensitive tasks help reduce exposure to cyber threats.

4. Data Protection and Privacy Compliance

Employees should understand how to handle sensitive data, comply with regulations such as GDPR or HIPAA, and report potential data breaches promptly.

5. Incident Reporting and Response

Clear protocols for reporting suspicious activity or security incidents enable swift action and minimize potential damage.

Best Practices for Implementation

To maximize the effectiveness of cybersecurity training, organizations should consider the following best practices:

- **Make Training Ongoing:** Cyber threats evolve constantly. Regular updates, refresher courses, and timely alerts help keep employees informed and vigilant.
- **Customize Content by Role:** Tailor training to specific job functions. For example, finance teams may need additional guidance on wire fraud, while developers should be trained on secure coding practices.
- **Use Interactive and Engaging Formats:** Gamified modules, videos, and quizzes enhance retention and make learning more enjoyable.
- **Measure and Improve:** Track participation, assess knowledge through testing, and analyze incident reports to identify gaps and refine the program.

Fostering a Culture of Cybersecurity

Cybersecurity training is most effective when backed by a strong security culture. Leadership must lead by example, promote best practices, and communicate the importance of security across the organization.

When employees feel supported, they're more likely to take ownership of their role in protecting the company.

Building a security-first culture means weaving cybersecurity into daily operations from onboarding to team meetings, until it becomes second nature.

ADVANCED STRATEGIES TO LOCK DOWN YOUR BUSINESS LOGINS

Good login security works in layers. The more hoops an attacker has to jump through, the less likely they are to make it to your sensitive data.

HERE ARE SOME PRACTICAL TIPS TO MAKE SURE YOUR EMPLOYEES ARE PROTECTED.

Strengthen Password and Authentication Policies.

If your company still allows short, predictable logins or reuses passwords, you've already given attackers a head start. Here's what works better:

- Require unique, complex passwords for every account.
- Swap out traditional passwords for passphrases; easier for humans to remember, harder for machines to guess.
- Roll out a password manager so staff can store and auto-generate strong credentials.

Enforce multi-factor authentication (MFA) everywhere possible.

- Check passwords against known breach lists and rotate them periodically.
- Apply the rules across the board. Leaving one "less important" account unprotected is like locking your front door but leaving the garage wide open.

Reduce Risk Through Access Control and Least Privilege.

- The fewer keys in circulation, the fewer chances there are for one to be stolen.
- Keep admin privileges limited to the smallest possible group.
- Separate super admin accounts from day-to-day logins and store them securely.
- Give third parties the bare minimum access they need.

Secure Devices, Networks, and Browsers.

Your login policies won't mean much if someone signs in from a compromised device or an open public network.

- Encrypt every company laptop and require strong passwords.

- Use mobile security apps, especially for staff who connect on the go.
- Lock down your Wi-Fi.
- Keep firewalls active, both on-site and for remote workers.
- Turn on automatic updates for browsers, operating systems, and apps.

Protect Email as a Common Attack Gateway.

One convincing message, and an employee clicks a link they shouldn't. To close that door:

- Enable advanced phishing and malware filtering.
- Set up SPF, DKIM, and DMARC to make your domain harder to spoof.
- Train your team to verify unexpected requests.

Plan for the Inevitable with Incident Response and Monitoring.

Even the best defenses can be bypassed. The question is how fast you can respond.

- Incident Response Plan
- Vulnerability Scanning
- Credential Monitoring
- Regular Backups

Make Your Logins a Security Asset, Not a Weak Spot

You don't have to do it all overnight. Start with the weakest link right now, maybe an old, shared admin password or a lack of MFA on your most sensitive systems and fix it. Then move to the next gap. Over time, those small improvements add up to a solid, layered defense.

LEARN MORE



A HACKER'S KRYPTONITE IS MFA

In today's rapidly shifting cybersecurity landscape, one fact remains clear: hackers exploit weak defenses. As threats grow more advanced, organizations must adopt layered security strategies to safeguard data, systems, and identities. One of the most effective and accessible tools is Multi-Factor Authentication (MFA) a simple yet powerful way to block unauthorized access.

Often called a hacker's kryptonite, MFA adds a vital layer of protection that can stop attackers even if passwords are compromised.

UNDERSTANDING MFA: MORE THAN JUST A PASSWORD

- **Something you know** – A password, PIN, or answer to a security question.
- **Something you have** – A smartphone, hardware token, or authentication app.
- **Something you are** – Biometric data such as a fingerprint, facial recognition, or voice pattern.

Some organizations delay MFA adoption due to concerns about cost or user inconvenience. But today's MFA solutions are designed to be both user-friendly and affordable.

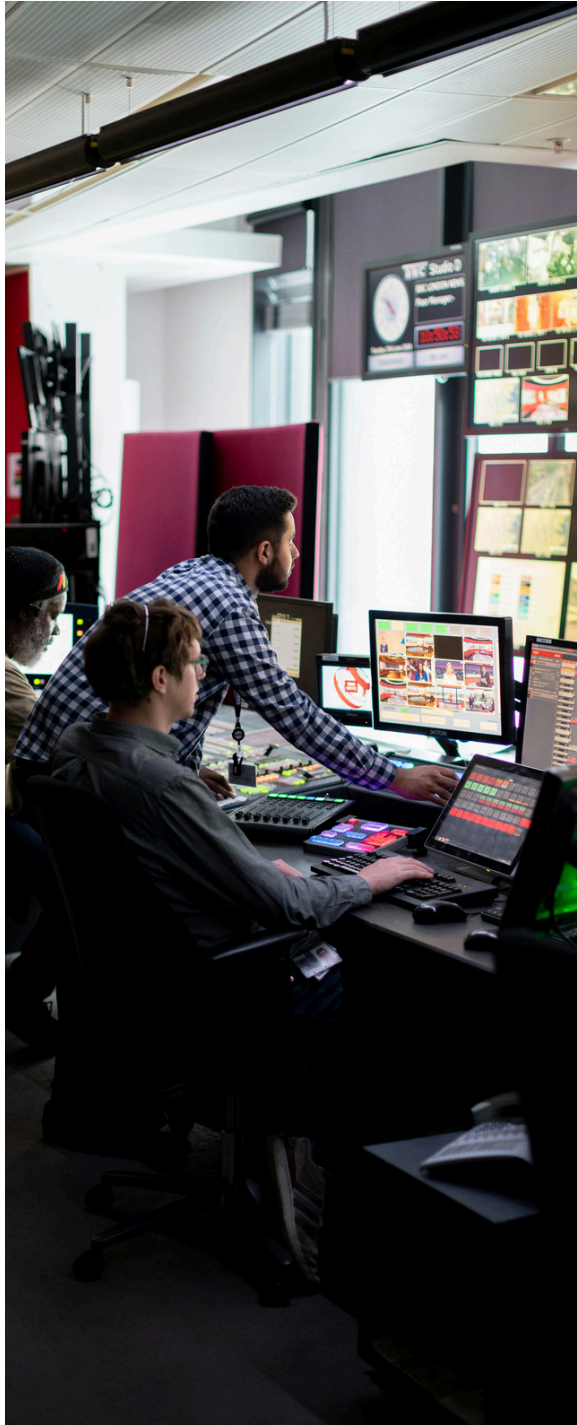
Platforms like Microsoft 365, Google Workspace, and Okta offer built-in MFA features that can be activated with minimal disruption.

The cost of implementing MFA is small, especially when compared to the financial and reputational damage a data breach can cause.

Implementing MFA: Strategic Considerations:

- **Enable MFA on Key Systems:** Apply MFA to email, cloud platforms, internal apps, and admin tools.
- **Use Adaptive Authentication:** Tailor MFA requirements based on user behavior, location, and device risk.
- **Train Employees:** Educate users on how MFA works and why it matters.
- **Audit Regularly:** Monitor MFA logs and settings to catch anomalies and ensure compliance.

Contact us to start building a future ready IT roadmap that turns your technology from a patchwork of tools into a true growth engine for your business.



TOP 10 CYBERSECURITY POLICIES EVERY COMPANY SHOULD HAVE

Password Management:

Bitwarden secures your business with encrypted, centralized password management—reducing risks from weak or reused credentials and enabling safe, efficient team access.

[Get Powerful](#)

Incident Response:

Sophos MDR delivers 24/7 threat detection and response, combining AI and expert analysis to stop attacks fast and keep your business secure.

[Get Protected](#)

Security Training:

Empower your team to recognize threats, reduce risk, and protect your business through practical, ongoing security education.

[Get Visibility](#)

10 Vendor Risk Management:



Evaluates and monitors third-party cybersecurity practices to prevent external threats.

[Get Secure](#)

- 1 Acceptable Use:**
Defines proper use of company devices and networks to prevent misuse and security risks.
- 2 Password Management:**
Enforces strong, unique passwords and multi-factor authentication to reduce breach risks.
- 3 Data Protection & Privacy:**
Regulates handling of sensitive data in compliance with laws like GDPR and HIPAA.
- 4 Incident Response:**
Outlines steps for detecting, containing, and recovering from security breaches.
- 5 Remote Access:**
Secures remote connections with VPNs, device standards, and public Wi-Fi restrictions.
- 6 Email & Communication:**
Promotes safe messaging practices to prevent phishing and data leaks.
- 7 Mobile & BYOD:**
Sets security standards for personal devices used for work, including encryption and remote wipe.
- 8 Access Control:**
Limits system access based on roles and managed.
- 9 Security Training:**
Requires ongoing employee education to reduce human error and build a security-first culture.

STOP ACCOUNT HACKS: THE ADVANCED GUIDE TO PROTECTING YOUR SMALL BUSINESS

Stop Account Hacks: The advanced guide to protecting your small business

Sometimes the first step in a cyberattack isn't code. It's a click. A single login involving one username and password can give an intruder a front-row seat to everything your business does online.





- **One Click Can Be Costly:** A single stolen login can expose your entire business. Credentials are often the easiest way in.
- **Small Businesses Are Prime Targets:** Nearly half of small businesses face cyberattacks, and stolen passwords are a leading cause.
- **Strong Passwords & MFA Are Essential:** Use long, unique passphrases and enforce multi-factor authentication across all accounts.
- **Limit Access with Least Privilege:** Only give users the access they need. Restrict admin rights and separate critical accounts.
- **Secure Devices and Networks:** Encrypt laptops, use strong Wi-Fi settings, and keep software updated to block entry points.
- **Email Is a Common Attack Path:** Deploy phishing filters, secure your domain, and train staff to spot suspicious messages.
- **Monitor and Respond Quickly:** Have an incident response plan, scan for vulnerabilities, and monitor for leaked credentials.
- **Backups Are Your Safety Net:** Keep secure, tested backups of critical data to recover quickly from breaches.
- **Treat Login Security as Ongoing:** Continuously improve your defenses—start with the weakest link and build from there.

Thank You!

Thank you for reading this month's cybersecurity update. We hope you found a few practical insights to help strengthen your digital defenses and make your technology work smarter for you.

If you ever have questions or need a second opinion on any cybersecurity matter, our team is just a call or email away, ready to support your business with expert guidance.

CONTACT AN EXPERT

-  (330) 800-2186
-  everythingit@virtualdataworks.com
-  virtualdataworks.com
-  475 Wolf Ledges Parkway Akron, Ohio 44311

