

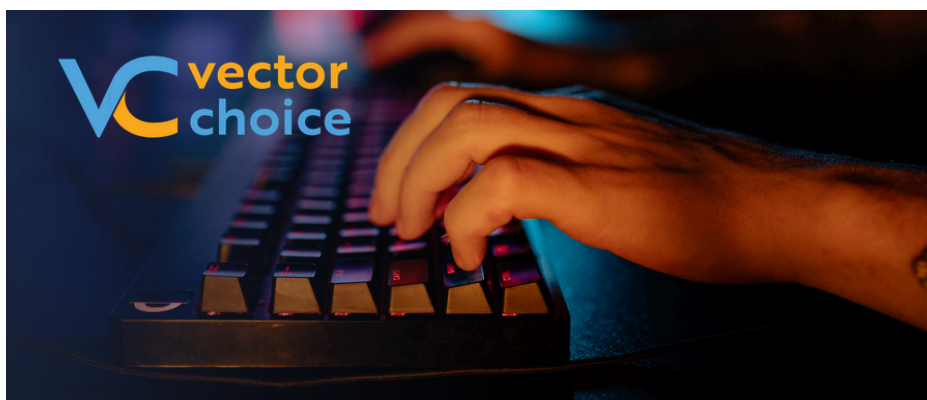
Stay Informed | Stay Secure | Stay Ahead

TECHNOLOGY TIMES

Cybersecurity Awareness Month: Building Layered Protection for Your Business

October is Cybersecurity Awareness Month, and this year we're focusing on what layered security really means. Cybersecurity isn't about one perfect tool — it's about building multiple layers of protection so when one layer is tested, others catch what slips through. This issue breaks down what layered cybersecurity looks like, why your team is your first line of defense, and how risk assessments help you understand where you stand.

What Layered Cybersecurity Actually Means



If someone told you they could secure your business with one product, they'd be overselling. Real cybersecurity means layering protection across your people, processes, and technology:

- **Endpoint Protection:** Antivirus, EDR, and device management for every device on your network.
- **Network Security:** Firewalls, secure Wi-Fi, segmentation, and monitoring.
- **Email Security:** Filtering and anti-phishing tools to stop the most common entry point for attacks.
- **Identity & Access Management:** MFA, password policies, and role-based access controls.
- **Backup and Recovery:** Regular, tested backups so you can recover without paying a ransom.
- **User Awareness and Training:** Ongoing training reduces the risk of human error.

No single layer is perfect — but together, they create a security posture that's much harder to breach.

EMPLOYEE SPOTLIGHT

Employee of the Month:
Rachel Fisher



Rachel Fisher has been named our September Employee of the Month! Rachel's adaptability, exceptional customer service, and dedication to creating a positive client experience set her apart. In a fast-paced environment, she consistently rises to challenges, supports her team, and exemplifies the values that make Vector Choice successful. Congratulations, Rachel!

Tech Genius of the Month:
Jordan Fussell



Jordan Fussell has been recognized as our September Team Member of the Month! Jordan's adaptability, exceptional service mindset, and focus on creating a great client experience have made a significant impact. He consistently handles challenges with professionalism, collaborates effectively with his team, and helps drive success for both our clients and Vector Choice. Congratulations, Jordan!

Gadget of the Month

ASUS - ZenScreen 16" FHD+ IPS Portable Monitor

This 16:10 display provides more viewing area, making it the ideal secondary display to extend workspace for hybrid workers. With an autorotation feature, it gives ZenScreen the versatility to be used in either landscape or portrait orientation. Also, with a power pass-through feature and USB-C ports, you can have two-way power delivery function that offers flexibility on the go



The Human Element: Your First Line of Defense

You can have the best firewall, the most advanced email filtering, and perfectly configured endpoint protection and still get breached because someone clicked a link they shouldn't have.

It's not about blaming your team — it's recognizing that attackers know people are often the easiest way in. Phishing emails are designed to look legitimate, and social engineering tactics exploit trust, urgency, and distraction. That's why security awareness training is just as important as the technology you deploy.

What Effective Security Training Looks Like:

- Regular phishing simulations that help employees recognize suspicious emails in a low-stakes environment
- Real-world examples of social engineering tactics, not just generic warnings
- Clear guidance on what to do when something looks wrong, who to contact, and how to report it
- Short, practical training sessions that fit into busy workdays instead of long annual courses
- Recognition and reinforcement for employees who catch and report potential threats

When your team knows what to look for and feels comfortable reporting suspicious activity, they become part of your security strategy, not a weak point in it.

At Vector Choice, we help businesses build security-aware cultures, not just security-aware systems. If you'd like to talk about security training options that actually stick, we'd be happy to walk you through it.

Cybersecurity Risk Assessment: What It Is and Why It Matters

Most businesses don't know exactly where their security gaps are until something goes wrong or until someone looks for them on purpose.

That's what a cybersecurity risk assessment does. It's a structured review of your technology, policies, and practices designed to identify vulnerabilities, evaluate risk, and prioritize what to fix first.

A good risk assessment typically includes:

- A review of your network security, endpoint protection, and access controls
- An evaluation of your backup and disaster recovery plans
- An analysis of your email security and phishing risk
- A check of your security policies, documentation, and incident response procedures
- A clear report that explains what was found, why it matters, and what to do next



Think of it like a physical for your IT environment. You're not waiting for symptoms to show up, you're proactively checking for issues before they become bigger problems.

For businesses in regulated industries, healthcare, finance, legal, and accounting. Risk assessments also support compliance requirements. Auditors, insurers, and regulators increasingly expect businesses to demonstrate that they understand their risk profile and have a plan to manage it. Even if you're not regulated, a risk assessment gives you clarity. You'll know where you stand, what your biggest exposures are, and how to prioritize your security budget.

Tech Tips You Can Use Right Now: September Recap

1

Beware of QR Code Phishing

Verify the source before scanning any QR code, and check the URL it opens before entering credentials.

2

Check Your App Permissions

Review what data and device access your apps can reach, and revoke anything that isn't necessary.

3

Use App-Specific Passwords

Generate unique passwords for individual apps instead of reusing your main account password.

4

Report Suspicious Activity

Flag anything unusual right away. Early reporting keeps a small issue from becoming a big one.

Want the October tech tips before next month's recap?

Sign up for our weekly tech tip emails now by scanning the QR code below:



Upcoming Webinar for November

The 12 Ways of Phishing



The 12 Ways of Phishing

A Phishing Email in Your Inbox

Traditional phishing emails designed to trick employees into clicking malicious links or opening attachments.

Two Fake Logins

Microsoft 365, Google, banking, and other cloned login pages built to steal usernames and passwords.

Three Urgent Requests

"Your account will be disabled." "Payment is overdue." "Respond immediately." How attackers weaponize urgency.

Four Spoofed Senders

Emails that appear to come from your CEO, CFO, vendor, bank, Microsoft, or another trusted source.

FIVE STOLEN CREDENTIALS!

How credential harvesting works—and what criminals do with passwords after they steal them.

Six Texts a-Scamming

Smishing: phishing through SMS and mobile messaging, including fake delivery notices, MFA alerts, and account warnings.

Seven Voices Calling

Vishing: phone-based social engineering—and how AI-generated voices are making fraudulent calls more convincing.

Eight QR Codes Scanning

Quishing: malicious QR codes that bypass the normal visual cues employees have learned to watch for in email.

Nine Executives Impersonated

Business Email Compromise (BEC), executive impersonation, fake wire requests, payroll changes, and fraudulent gift-card requests.

Ten Vendors Billing

Vendor impersonation, fake invoices, altered ACH instructions, and compromised vendor email accounts.

Eleven MFA Requests

MFA fatigue, push bombing, fake authentication requests, and techniques attackers use to get around MFA.

Twelve AI Phishes

How generative AI, deepfakes, voice cloning, personalization, and automation are making phishing attacks harder to recognize.

How to Keep the Grinch Out of Your Network

Wrap it up with "**12 Days of Defense**"...a practical checklist covering security awareness training, phishing simulations, MFA/passkeys, email security, conditional access, verification procedures for financial changes, DMARC / SPF / DKIM, endpoint protection, monitoring, and incident-response procedures.

