

BUILDING A CYBER STRONG CULTURE

Empowering every employee to be the first line of defense



THIS MONTH'S TOPICS:

Leading With Security

How Culture Shapes Safety

Becoming Cyber Strong

Positive Cyber Habits to Adopt

Scam of the Month:

Delivery Scams

The Cost of Weak Cyber Habits

Very Scary Statistics

October is Cybersecurity Awareness Month, and this issue of our newsletter focuses on building a Cyber Strong Culture, one where every click, conversation, and choice contributes to a safer digital workplace.

Inside, we'll explore how to strengthen your cyber habits, avoid costly mistakes, and stay alert to the latest scams. Learn how small, consistent actions can make a big impact, see why poor habits can be dangerous, and uncover how criminals use scams to trick even the most careful employees. Finally, we'll highlight how leadership and teamwork drive lasting cyber resilience across every organization.

LEADING WITH SECURITY

HOW CULTURE SHAPES SAFETY

Cybersecurity doesn't start with technology. It starts with leadership.

When managers, executives, and team leaders make cybersecurity a visible priority, employees follow their example. A strong cyber culture isn't built through fear or enforcement, but through trust, communication, and consistency.

Creating a culture of security means making safe practices part of everyday work instead of an afterthought. From password hygiene to reporting incidents, leaders shape how seriously teams take cybersecurity. Every decision, policy, and conversation helps define the organization's security mindset.



WHAT LEADERSHIP IN CYBERSECURITY LOOKS LIKE

Leaders shape culture through action. When management practices good cybersecurity, such as using MFA, completing training, and reporting suspicious activity, employees follow.

Create an environment where employees feel safe reporting mistakes or suspicious activity. The faster an issue is reported, the smaller the impact.

Replace fear with empowerment. When employees understand why security matters, they become active defenders rather than passive rule followers.

Celebrate those who identify threats or take initiative. Recognition reinforces that cybersecurity is a shared success, not just an IT task.

STRENGTHEN YOUR CYBER CULTURE THIS MONTH

Talk About Security in Every Team Meeting
Start small — add a one-minute cybersecurity reminder or success story to team meetings. Consistent communication keeps awareness high and normalizes security discussions.

Recognize and Reward Awareness
Give a quick shoutout to employees who report suspicious emails, complete training early, or share helpful cybersecurity tips. Positive reinforcement builds engagement and momentum.

Lead by Example
Show your team that cybersecurity isn't optional. Use MFA, complete your own training on time, and follow data handling policies carefully. Your actions set the tone for the entire organization.



BECOMING CYBER STRONG

POSITIVE CYBER HABITS TO ADOPT



THINK BEFORE YOU CLICK

Pause and inspect links, attachments, and messages before taking action.



USE STRONG, UNIQUE PASSWORDS

Avoid reusing passwords across accounts. Consider using a reputable password manager.



ENABLE MULTI-FACTOR AUTHENTICATION

MFA adds a powerful layer of protection that keeps your accounts safe even if a password is stolen.



KEEP SOFTWARE AND DEVICES UPDATED

Regular updates patch vulnerabilities that cybercriminals exploit.



LOCK YOUR DEVICES WHEN AWAY

Even brief moments away from your desk can create opportunities for unauthorized access.



REPORT SUSPICIOUS ACTIVITY IMMEDIATELY

Reporting early helps prevent incidents from spreading.



SCAM OF THE MONTH: DELIVERY SCAMS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

It was a typical Tuesday when Sarah, a busy office manager, received a text that looked like it came from a well-known shipping company. The message said her package couldn't be delivered and included a link to "reschedule delivery." Thinking it might be the printer toner her team had ordered, she clicked the link. The page looked legitimate—complete with the company's logo—and asked her to confirm her address and pay a small redelivery fee. Within minutes, Sarah's credit card was charged hundreds of dollars for purchases she didn't make.

Later that day, Sarah learned the company never sent the text—it was a delivery scam designed to steal personal and payment information. Scammers often impersonate shipping companies during busy seasons, knowing most people expect packages and won't think twice about clicking.



DID YOU SPOT THE RED FLAGS?

- ▶ The message requested a "redelivery fee." Legitimate shipping companies don't request additional payments through text or email links.
- ▶ The text included a link to "reschedule delivery," which led to a fake website.

HOW TO PROTECT YOURSELF



If you receive a text or email about a delivery, don't click any links. Instead, enter your tracking number on an official website or app.



Never provide personal or payment information through a link you didn't initiate.



THE COST OF WEAK CYBER HABITS



VERY SCARY STATISTICS



The global average cost of a data breach rose to **\$4.88 million** in 2024, marking a ~10% increase over the previous year.

Approximately **88%** of cybersecurity breaches have an element of human error (i.e., weak habits, mistakes, or lapses).

Cybercrime is predicted to cost the world **\$10.5 trillion USD** in 2025, according to Cybersecurity Ventures.

In 2024, organizations were exposed to **600 million** cyberattacks per day (global estimate).

It's estimated that cybercriminals earn **\$1.5 trillion** annually by cybercrime activities.

46% of all cyber breaches affect businesses with **fewer than 1,000** employees.

