THE NEW CYBER REALITY

How threats evolved, myths prevailed,
and culture became the strongest defense

THIS MONTH'S TOPICS:

Evolution of Cyber Threats
How attacks changed over the years

Cybersecurity Myths
Common beliefs that put you at risk

Scam of the Month:
One-Time Password Scams

Fostering Cyber Culture
Simple ways to build safer habits

Cybersecurity isn't what it used to be, and that's why it's so important to stay grounded in what's real. As technology has evolved, so have the tactics criminals use. In this issue, The New Cyber Reality takes a quick look at how cyber threats have changed and why understanding that evolution helps us respond smarter.

We'll also clear up some of the most common cybersecurity myths that can lead to risky decisions, even for well-meaning employees. Finally, we'll explore how organizations build a strong cybersecurity culture. The best defense is consistent habits, shared accountability, and a team that knows how to stay vigilant.

THE EVOLUTION OF CYBER THREATS OVER THE YEARS

Cyber threats have gotten smarter, faster, and more personal. Years ago, many attacks were easy to spot. They contained broken English, suspicious attachments, and obvious "you won!" messages. Today, criminals copy real brands, use familiar tools (texting, social media, and email), and design scams to feel routine—like signing in, verifying an account, or approving a request.

The good news? While tactics evolve, the goal is usually the same. Steal credentials, steal money, or steal access. Knowing how threats have changed helps you recognize the patterns before you click, reply, or approve.

THEN VS NOW

Early days: High Volume, Mass Attacks

- Attackers sent mass emails to anyone and everyone
- Common lures: fake prizes, chain emails, "virus alerts," and sketchy attachments
- Easy tells: odd formatting, generic greetings, and mismatched sender addresses

Today: Targeted and Timed

- Attackers tailor messages using info from social media, data breaches, and company websites
- Common lures: payroll updates, invoice/payment changes, password resets, delivery notices, and HR "urgent" requests
- Harder tells: realistic branding, clean writing, and "perfect timing" (during busy hours, travel, year-end, tax season)

CONSISTENT PATTERNS

- **Urgency:** "Do this now"
- **Authority:** "I'm IT/your boss/your bank"
- **Convenience:** "Just click/sign in/confirm this code"
- **Fear or excitement:** "Security issue" or "You've won"

CYBERSECURITY
Myths and Misconceptions

MYTH #1: “I’m not important enough to be targeted.”

Most attacks are automated and aimed at anyone who might click, reply, or reuse a password. Assume you’re a potential target, always.

MYTH #2: “My device looks fine, so nothing’s wrong.”

Many compromises are silent—no pop-ups, no slowdown, no obvious “virus.” Keep software updated, use security tools, and report suspicious messages.

MYTH #3: “MFA protects me completely.”

MFA is a huge layer of protection, but it’s not foolproof. MFA fatigue prompts, one-time passcode (OTP) scams, and stolen session cookies can still bypass MFA.

MYTH #4: “Only links are dangerous. Attachments are fine.”

Malicious attachments and QR codes can be just as risky. Some attacks start with enabling macros or opening a file that looks routine.

MYTH #5: “A strong password is enough.”

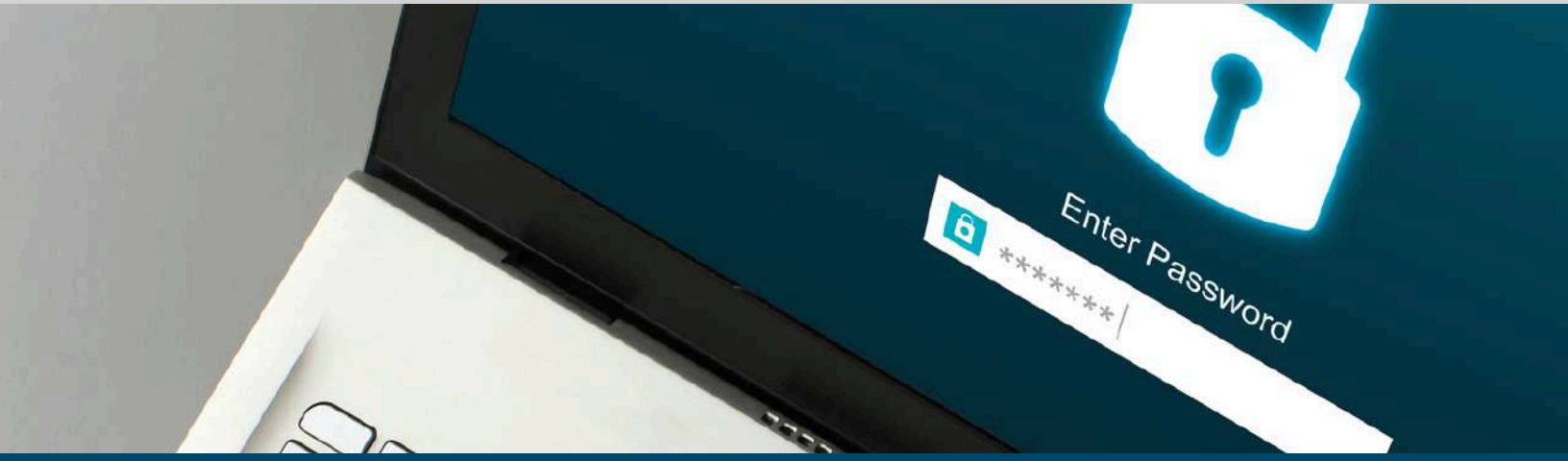
Strong passwords help, but if you reuse them and one site gets breached, attackers can try that password everywhere.

SCAM OF THE MONTH: ONE-TIME PASSWORD SCAMS

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

Maya's phone buzzed: "BankSecure: Password changed. If this wasn't you, reply NO." She panicked and replied. A second text followed: "To secure your account, enter the one-time code we just sent." Then her phone rang. "Hi Maya, this is Daniel from the bank's fraud team," the caller said. He sounded official, urgent, and reassuring. "I can stop the transfer, but I need that code for verification." Maya hesitated, but it sounded convincing. She read the six digits aloud.

The caller thanked her and hung up. Seconds later, new alerts appeared. A payee was added, and a transfer was submitted. Maya called her bank using the number on her card and learned the truth: The code authorized the scammer to log into her account. Shaken, she promised herself she'd always hang up and call back using a trusted number, no matter how urgent the caller sounded.



DID YOU SPOT THE RED FLAGS?

- Real banks and support teams won't call you and ask you to read or share a one-time code or password.
- The "fraud alert" and phone call created pressure to act fast, making it less likely Maya would pause and refuse to hand over that information.

HOW TO PROTECT YOURSELF

- Never share one-time codes or passwords. If someone asks for that information, assume it's a scam.
- Always verify requests through a trusted channel. Contact the company using the number on your card, the official website, or the app.

How Organizations Foster
A CYBERSECURITY CULTURE

A strong cybersecurity culture is when secure behavior is the default, not an extra step people skip when they're busy. It's built through clear expectations, leadership support, and systems that make it easy to do the right thing. The goal is to create habits that reduce risk every day.

What do great security cultures have in common?

Leaders model the behavior

- Executives and managers follow the same rules (MFA, reporting, secure sharing)
- Security is talked about as a business priority

Security is simple and practical

- Policies are short, realistic, and tied to real-world examples
- Tools reduce friction (password managers, MFA apps)

Training is ongoing

- Short micro-trainings and quick reminders are the norm
- Topics match current threats and are both informative and easy to understand

People are rewarded for reporting

- Employees are encouraged to report suspicious messages, even if they clicked
- Reporting is framed as helpful, not embarrassing

Access is managed intentionally

- Employees only get the access they need (least privilege)
- Offboarding is fast and consistent (accounts disabled immediately, credentials rotated)

Vendors and partners participate

- Third parties follow security requirements and are reviewed regularly
- Invoice/payment changes require verification steps to prevent fraud