

# **WORKPLACE HANDOUT: Cybersecurity is Everyone's Job**

October is National Cybersecurity Awareness Month

## **The Core Message: You Are the First Line of Defense.**

Cybercriminals don't just target computer networks; they target the **people** operating them. A single accidental click on a malicious link can compromise our entire company's data, disrupt our operations, and expose sensitive employee or customer information. Staying cyber-safe is just like using physical PPE—it protects you, your coworkers, and our business.

---

## **1. The 4 Golden Rules of Workplace Cyber Safety**

You don't need to be an IT expert to keep our workplace secure. Consistently practicing these four simple behaviors stops the vast majority of cyber-attacks:

- **Think Before You Click (Phishing Defense):** Be highly suspicious of urgent or unexpected emails, texts, or direct messages. If an email demands immediate action, asks you to change a password, or requests that you download an unexpected invoice, verify it with the sender through a separate phone call or standard chat channel first.
  - **Use Strong, Unique Passwords:** Never reuse passwords across multiple accounts. A strong password is a phrase that is long (at least 14 characters) and combines uppercase letters, lowercase letters, numbers, and symbols.
  - **Turn on Multi-Factor Authentication (MFA):** Whenever available, enable MFA (sometimes called two-step verification). This adds an extra layer of security by requiring a code from your phone or an authenticator app, ensuring that even if a hacker steals your password, they still can't log in.
  - **Keep Software Updated:** Don't click "remind me later" on system updates. Keeping your operating system, web browsers, and work applications updated ensures that critical security patches are installed to block known software vulnerabilities.
- 

## **2. Spotting the Red Flags of an Attack**

Cybercriminals use psychology to trick us. Watch out for these common workplace manipulation tactics:

- **Artificial Urgency:** Emails containing phrases like *"Action Required Immediately!"* or *"Your account will be suspended in 2 hours."*
  - **Mismatched Sender Addresses:** The display name says it's your boss or a trusted vendor, but the actual email address after the name looks strange or uses a slightly misspelled domain (e.g., *boss@compnay.com* instead of *company.com*).
  - **Unusual Requests:** Coworkers or executives suddenly asking you to buy gift cards, wire funds, or bypass standard operational authorization procedures via an email or text message.
- 

## **3. What to Do If You Suspect a Threat**

- **Report It Immediately:** If you receive a suspicious email, do not forward it to your coworkers. Use your company's designated spam reporting tool or notify your IT supervisor immediately.
- **Disconnect if Compromised:** If you accidentally clicked a link or entered your credentials into a suspicious page, disconnect your device from the Wi-Fi/network cable immediately to stop the spread of potential malware, and notify management.
- **Better Safe Than Sorry:** It is always better to report a false alarm than to stay silent about a real security breach.