



Fraud Is On The Rise; Is Your Company Prepared?

CYBERSECURITY STARTS WITH PEOPLE

Your employees are more than just technology users. They are **your first line of defense against cyber threats**. Every email opened, link clicked, and file shared presents a **potential risk or an opportunity** to protect your organization.

WHY CYBER HYGIENE TRAINING MATTERS

- ◆ Cyber threats continue to grow in **frequency and sophistication**.
- ◆ Human error remains one of the **leading causes of security incidents**.
- ◆ Well-trained employees can **identify and prevent attacks before they escalate**.

BUILD A CULTURE OF CYBER AWARENESS

Every employee, regardless of role, must understand:

- ◆ How to recognize phishing and social engineering.
- ◆ The importance of strong passwords and Multi-Factor Authentication (MFA).
- ◆ Safe handling of sensitive company and customer data.
- ◆ Secure practices when working remotely or in public spaces.

Cybersecurity is a shared responsibility across the entire organization. A small investment in training can prevent costly breaches, reputational damage, and regulatory exposure.

TAKE ACTION TODAY

- ◆ Implement regular, structured cybersecurity training.
- ◆ Reinforce key messages through ongoing communication.
- ◆ Recognize and reward employees who demonstrate strong cyber habits.

REMEMBER:

Cybersecurity awareness is critical regardless of company size. Whether your organization has 3 employees or 300, every individual plays a role in protecting systems, data, and customers.

Smaller teams often believe they are less likely to be targeted; however, cybercriminals frequently exploit this mindset. Organizations of all sizes must ensure employees are trained to recognize threats, follow secure practices, and respond appropriately.



Awareness is your best defense against fraud.

