PROVIDENCE BANK & TRUST

# security awareness

INFO TO KNOW

All organizations – from large and small businesses to healthcare providers, academic institutions, government agencies and civil society – can experience data breaches or be targets of cybercrime, which can result in stolen intellectual property, theft of personal information or – if our critical infrastructure is attacked – a disruption to our way of life.

Creating a culture of cybersecurity in the workplace through efforts like employee education, training and awareness and by emphasizing risk management, resistance and resilience will help combat cyber crime.

## National Cyber Security Awareness Month

### From the Break Room to the Board Room: Creating a Culture of Cybersecurity in the Workplace

The best security technology in the world can't help you unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. This will involve putting practices and policies in place that promote security and training employees to be able to identify and avoid risks.

**Talk to Your Employees About**

Keeping a clean machine: Your company should have clear rules for what employees can install and keep on their work computers. Make sure they understand and abide by these rules. Unknown outside programs can open security vulnerabilities in your network.

Following good password practices: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces! Additionally, having separate passwords for every account helps to thwart cybercriminals. At a minimum, they should separate work and personal accounts and make sure that critical accounts have the strongest passwords. Finally, writing down passwords and keeping them in a safe place away from the computer and enabling two-step authentication are other important ways to secure accounts.

**A computer network assessment will help you begin a cybersecurity plan to mitigate the largest risks to your business.**

**Most experts recommend that businesses start by having a strategic approach to cybersecurity. This strategic approach should include plans to secure existing systems and keep your business secure going forward.**

**Your best sources of guidance are your Internet Service Provider (ISP) and software providers. Many ISPs have services devoted to their business customers. Explore what's available from them and how they can help. The provider of your security and other software can also be of assistance and may have special services for small businesses.**

When in doubt, throw it out: Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email.

Backing up their work: Whether you set your employees' computers to back up automatically or ask that they do it themselves, employees should be instructed on their role in protecting their work.

Staying watchful and speaking up: Your employees should be encouraged to keep an eye out and say something if they notice strange happenings on their computer.

## Training Your Employees

Training employees is a critical element of security. They need to understand the value of protecting customer and colleague information and their role in keeping it safe. They also need a basic grounding in other risks and how to make good judgments online.

Most importantly, they need to know the policies and practices you expect them to follow in the workplace regarding Internet safety.

**Help the authorities fight cybercrime:**

If your business has been victimized by a cyber attack, you should notify the appropriate authorities. This gives you a chance to recoup any losses and ensure that the attackers are brought to justice.

#CyberAware

Content provided by staysafeonline.org.