PROVIDENCE BANK & TRUST

security awareness

INFO TO KNOW

Cybercrime has become too common in our connected world. While online crime is often associated with hackers stealing personal information for monetary gain, crime on the Internet takes many forms. Cybercrime can include everything from organizational data breaches to consumer issues like identity theft, cyber-stalking, harassment and bullying to child sexual exploitation and abuse to online radicalization, violence and recruitment to terrorist networks. Fighting cybercrime requires a high level of collaboration among law enforcement, government agencies, the private sector and the general public.

National Cyber Security Awareness Month

Recognizing and Combating Cybercrime

Most households now run networks of devices linked to the Internet, including computers, laptops, gaming devices, TVs, tablets, and smartphones that access wireless networks. To protect your home network and your family, you need to have the right tools in place and confidence that family members can use the Internet safely and securely.

The first step is to Keep a Clean Machine and make sure all of your Internet-enabled devices have the latest operating system, web browsers and security software. This includes mobile devices that access your wireless network.

Secure Your Wireless Router

A wireless network means connecting an Internet access point – such as a cable or DSL modem – to a wireless router. Going wireless is a convenient way to allow multiple devices to connect to the Internet from different areas of your home. However, unless you secure your router, you're vulnerable to people accessing information on your computer, using your Internet service for free and potentially using your network to commit cybercrimes.

Here are ways to secure your wireless router:

Change the name of your router: The default ID - called a service set identifier" (SSID) or "extended service set identifier" (ESSID) – is assigned by the manufacturer. Change your router to a name that is unique to you and won't be easily guessed by others.

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post. Have your family follow these tips to safely enjoy social networking:

- Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.
- Know and manage your friends.
- Be honest if you're uncomfortable.
- Know what action to take.

Change the pre-set password on your router: When creating a new password, make sure it is long and strong, using a mix of numbers, letters and symbols.

Review security options: When choosing your router's level of security, opt for WPA2, if available, or WPA. They are more secure than the WEP option.

Create a guest password: Some routers allow for guests to use the network via a separate password. If you have many visitors to your home, it's a good idea to set up a guest network.

Use a firewall: Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for attempts to access your system and blocking communications with sources you don't permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

CyberAware

Help the authorities fight cybercrime:

Report stolen finances, identities and cybercrime to:

http://www.ic3.gov (the Internet Crime Complaint Center)

http://www.onguardonline.gov/file-complaint (the FTC).

Content provided by staysafeonline.org.