PEAPACK-GLADSTONE BANK

Private Banking since 1921

Cybersecurity In The Home

3 Steps Households Can Take

The COVID-19 pandemic forced millions of Americans to embrace working from their own home; a concept they had limited or no experience with at the time. And while many employees have returned to the office, a recent University of Chicago study found that 72% of those workers surveyed would like to continue working from home for at least 2 days a week, and 32% said they would like to work from home permanently. In this new reality, having your household safe and secure from cyber threats needs to be a top priority.

In this increasingly wireless world, the steps households should take in terms of cybersecurity have changed. Most homes now run networks of devices linked to the internet, including computers, gaming systems, TVs, tablets, and smartphones that access wireless networks. Thus, having the right tools in place will instill confidence that your family members can use the internet safely and securely for personal and work-related endeavors.

Below are 3 steps households can take to better protect themselves against cyber-attacks:

Secure Your Wireless Router

Using a wireless router is an increasingly convenient way to allow multiple devices to connect to the internet from different areas of your home. However, unless your router is secure, you risk the possibility of individuals accessing information on your computer, and worse, using your network to commit cybercrimes. Needless to say, all wireless devices using this router are vulnerable if your router is not protected. Some simple ways to secure this piece of hardware include changing the name of your router. The default ID is typically assigned by the manufacturer, so changing your router to a unique name that won't be easily guessed by others is a simple way to keep your router protected. Another important step is changing the preset passphrase on your router. Leaving the default password in place makes it significantly easier for hackers to access your network. In fact, according to NCA's 2021 Oh Behave! Report, only 43% of participants reported creating long and unique passwords for their online accounts "very often" or "always". Additionally, almost a third (28%) stated that they didn't do this at all. Embracing unique and strong passwords is a huge and simple step to securing your home from all types of cyber threats.

PEAPACK-GLADSTONE BANK

Private Banking since 1921

Cybersecurity In The Home

Install Firewalls and Security Software On All Devices

Firewalls are essential because they help keep hackers from using your device which otherwise could result in your personal information being sent out without your permission. They guard and watch for attempts to access your system while blocking communications with sources you don't permit. Installing a firewall on wireless routers is a necessity. Furthermore, make sure all devices that are connected to the wireless network have security software systems installed and updated. Many of these gadgets have automatic update features, so households should make sure they are on for all available technology. The most up to date security software, web browsers, and operating systems are the best defense against online threats such as viruses and malware.

Back Up All Household Data

While steps can be taken to avoid your network, devices and accounts being hacked or compromised, they can never be 100% effective. With this in mind, households need to embrace backing up data, especially as it relates to important information. Users can protect their valuable work, photos and other digital information by making electronic copies of important files and storing them safely. This can be done using cloud software in addition to manual storing devices like USBs. Regardless, storing data in an alternative location that is safe and secure provides another layer of protection. Taking simple, proactive steps to keep family, friends and yourself safe from cyber criminals inside your household should no longer be viewed as optional but rather a necessity. Between technological devices being introduced and updated at a rapid pace and employees continuing to embrace working from home in some capacity, everyone has an ethical responsibility to actively minimize the risks of breaches and attacks inside their home.