STAY CONNECTED AND CAUTIOUS

In a remote or hybrid workplace, employees rely on connected devices from their home office to do their jobs. According to recent data, smart home systems are set to rise to a market value of $157 billion by 2023, and the number of installed connected devices in the home is expected to increase 70% by 2025. In this new normal, smart devices and online safety are a must. Below are some tips for securing those devices and staying safe online.

Smart Devices Need Smart Security

It's important to make cybersecurity a priority when purchasing a connected device. When setting up a new device, be sure to set up the privacy and security settings right away. Consider limiting your device's ability to track and store location data so you don't unknowingly expose your location.

Put Cybersecurity First

Always make sure you're taking the proper security measures with your work devices. FNF deploys multiple layers of security to protect our systems, but that doesn't absolve your obligations to exercise cybersecurity best practices to keep FNF safe. Some precautions include performing regular software updates and enabling MFA whenever accessing a connected device, email or account.

Make Passwords Long and Strong

Generic passwords are the easiest to hack. Create long, unique passwords, and always combine capital and lowercase letters with numbers and symbols to create the most secure password. If you need help remembering and storing your passwords, don't hesitate to turn to a password manager for assistance.

Practice Caution in Public

While working from home, you may want to get a change of scenery and work from a coffee shop or another type of public space. While this may keep the day from becoming monotonous, working in a public setting can subject you to new cybersecurity tshreats. If you're working in a public setting, always
keep your laptop and device screens out of view of others, and never use public computers to access sensitive material

Turn Off Your WiFi and Bluetooth

When WiFi and Bluetooth are on, hackers can connect and track your whereabouts. To stay as safe as possible, always switch off WiFi and Bluetooth when you are not actively using them. It's a simple step that can help alleviate tracking concerns and security incidents.
Staying safe online is an active process that requires thoughtfulness at every stage, from purchasing and setting up a new device to making sure that your day-to-day activities are not putting you or your company at risk. By following these recommendations, you are helping to keep yourself and your company safe from malicious online activity. For more information about cybersecurity, please visit https://www.cisa.gov/national-cyber-security-awareness-month.