Prioritizing Cybersecurity *in a* Hybrid Workplace

CYBERSECURITY AWARENESS MONTH

In this day and age, employees are more connected than ever. The hybrid workplace is here to stay, and for employees, this means relying on connected devices from their home office setups. 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 rise by a staggering 70% by 2025. In this new normal where smart devices and consequently online safety are a must, here are some tips for securing those devices.

1 Remember smart devices need smart security

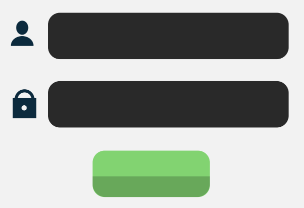
Make cybersecurity a priority when purchasing a connected device. When setting up a new device, be sure to set up the privacy and security settings on web services and devices bearing in mind that you can limit who you are sharing information with. Once your device is set up, remember to keep tabs on how secure the information is that you store on it, and to actively manage location services so as not to unwittingly expose your location.

2 Put cybersecurity first in your job

Make cybersecurity a priority when you are brought into a new role. Good online hygiene should be part of any organization's onboarding process, but if it is not, then take it upon yourself to exercise best practices to keep your company safe. Some precautions include performing regular software updates and enabling MFAs.

3 Make passwords and passphrases long and strong

Whether or not the website you are on requires it, be sure to combine capital and lowercase letters with numbers and symbols to create the most secure password. Generic passwords are easy to hack. If you need help remembering and storing your passwords, don't hesitate to turn to a password manager for assistance.

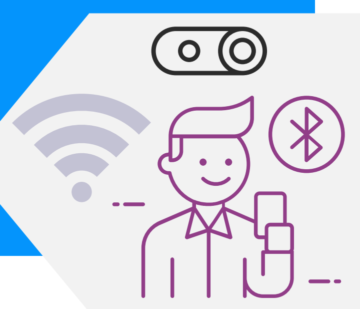


4 Never use public computers to log in to any accounts

While working from home, you may be tempted to change scenery and work from a coffee shop or another type of public space. While this is a great way to keep the day from becoming monotonous, caution must be exercised to protect yourself and your company from harm's way. Make sure that security is top of mind always, and especially while working in a public setting, by keeping activities as generic and anonymous as possible.

5 Turn off Wi-Fi and Bluetooth when idle

The uncomfortable truth is, when Wi-Fi and Bluetooth are on, they can connect and track your whereabouts. To stay as safe as possible, if you do not need them, switch them off. It's a simple step that can help alleviate tracking concerns and incidents.



These are just a few simple steps towards achieving the best online safety possible. Staying safe online is an active process that requires constant overseeing at every stage - from purchasing and setting up a device, to making sure that your day-to-day activities are not putting anyone at risk.

By following these steps, you are doing your part to keep yourself and your company safe from malicious online activity.

SOURCE
https://staysafeonline.org

CREATED BY
Security Service of Aruba

CYBERSECURITY AWARENESS MONTH

Vigilantia Diligentia Animus