PREVENTING A CYBER PANDEMIC: KEY SECURITY CONSIDERATIONS

Due to the global coronavirus pandemic, working from home has become commonplace. Nearly 85% of business leaders anticipate expanding remote work options beyond the pandemic. Yet, remote workers can inadvertently jeopardize an organization's security. As it stands, 45% of employees who are newly working from home haven't received any cyber security awareness training.

Concerns surrounding a cyber pandemic -which could move more quickly than a biological pandemic- are prompting leaders to leverage employee support when it comes to security. To reduce human error, and to mitigate the effects of a potential cyber pandemic, see below for a series of cyber security best practices to apply while working from home.

OBSERVE YOUR EMAILS.

The US Cybersecurity and Infrastructure Security Agency (CISA) recently reported an increase in phishing scams, and warned email users to be on the lookout for them. In unsolicited emails, avoid clicking on any links. In addition, email users should carefully consider whether to open email attachments. If an email promises you 'the latest facts about the coronavirus,' for example, opt to obtain information from trusted, government websites and news agencies instead. And prior to sending any money to a charity, be sure to verify the group's authenticity and to read the latest Federal Trade Commission reports on charity scams.

ENCRYPT DATA ON DEVICES.

Data encryption is an essential component of good cyber hygiene. It can protect the information on the device, and also protect any information transmitted to or from the device. Unless a cyber criminal possesses the decryption key, only an authorized user will be able to access the device.

SECURE YOUR VIDEO CONFERENCE CALLS.

During the first half of 2020, a rash of "Zoom bombings" plagued business meetings and personal video conferences. Since then, popular video conferencing platforms have made strides in improving their security. Some even offer end-to-end encryption. On your end, you can require authentication in order for users to join Zoom calls. You can do this by requiring participants to use a special password to access the call, and by admitting participants one-by-one from a virtual 'waiting room'. Experts suggest that meeting hosts 'lock' the call once it has commenced.

USE MULTI-FACTOR AUTHENTICATION (MFA).

With MFA, users must prove their identity by entering a pin sent to their mobile phones, or by answering a security question via email. This offers a second means of ensuring that those requesting access (to whatever) are who they claim that they are. Wherever possible, the use of multi-factor authentication should become standard practice.

UPDATE YOUR SOFTWARE WHEN PROMPTED.

As annoying as updates often are, using the latest software can help you ensure that a cyber attacker can't exploit a known vulnerability in the software. It's worth taking 10 minutes of your day to install the latest version and to restart your computer when prompted. That alone could save your organization millions in breach expenses.

Although we may not be able to avoid a global cyber pandemic, empowering employees to safeguard their company resources is the first step in preventing digital damage. Connect with your IT team to learn about additional cyber security best practices in the new era of remote work.