5 Ways Employees can Prevent Cyberattacks

June 9, 2021 Posted by Holly Mockus

While a long an ever-present threat to businesses, city government, schools, and hospitals, cybercriminals are now aggressively targeting manufacturers with increasing frequency. Here's how you can enlist your employees to help defend against these attackers.

According to the FBI's Cyber Division, even during the pandemic, cyberattacks rose by 400% to 4,000 attacks a day. This increase includes a refined focus on manufacturers. Around this time last year, the Manufacturers Alliance for Productivity & Innovation (MAPI) released a report with Deloitte that found 40% of manufacturers were victims of a cyberattack over 12 months.

Manufacturers are being walloped with ransom demands, particularly in the energy, transportation, and food sectors. And now the White House is warning corporate executives and business leaders to step up security measures to protect against ransomware attacks.

While infrastructure improvements are needed on a physical level to shore up security on devices and networks, we also know that some of the greatest vulnerabilities occur on the personal level where people interact with technology.

Cybercriminals rely on human error to gain entry to company systems. Luckily, there are routines and steps you can teach your employees to help protect them, your company, and your customers. While these tips may seem simple to some readers, the key (as always) is providing employees the proper training and refreshers.

Refresh Your Password Hygiene

Given the prominence of cyberattacks in the news, now's a great time to look at your password policies. Most companies require employees to change their passwords every 60 to 90 days and avoid using the same password for multiple accounts.

The strongest passwords are at least 12 characters long and include a mix of upper- and lower-case letters, symbols, and numbers. Of course, the trick isn't so much about creating a complex password. It's remembering it.

Here are a couple of tips to help. Use four to six random, unrelated words. Make sure they're not related to you. And don't use pet or street names. Make a mental image with the words to make them easier to remember. Now use symbols and numbers or capitalize the same letter of every word in this case. And throw in numbers and symbols. It might look something like this: *Coff33HatBicycl3!*

Another way to remember a complex password is to think of the first line of your favorite song or make up a sentence that you can remember. Now take the first letter of each word and mix in upper- and lower-case letters, numbers, and symbols. For example: Do*ILikeThisPassword?*.

As an added step to teaching password hygiene, include multi-factor authentication. If employees try to log in from another device or change their passwords, they will get a call or text to confirm that it's them making the change.

5 Ways Employees can Prevent Cyberattacks

Keep Software Programs Updated

Make it a common practice for employees to keep their applications updated. For example, it's easy to check to see if you have the latest version of Google Chrome. Just pull down the "help" menu and go to "About Google Chrome." It will automatically check to see if you have latest version. Other software programs offer similar procedures.

Other applications might have to be updated by IT. These updates will include patches to address newly discovered vulnerabilities. It's easy for cybercriminals to test your networks to determine your update status. Older versions offer unchecked vulnerabilities to exploit.

Backup Copies of Data and Applications

With ransomware, it's easy for cybercriminals to lock down your data and your applications until you meet their financial demands. However, cloud-based backup and disaster recovery programs make it easy to backup data automatically and restore your operations to any point in time. It's also important to teach employees how to back up their data to your cloud or approved devices.

Keep Personal and Business E-Mail Separate

Help employees understand why it's essential to keep their work and personal email separate and to keep their social media activities on their personal devices whenever possible. An entire network can be exposed to malware by simply clicking into a cat video over a company computer. Logging into personal shopping sites on work devices or searching for something as innocent as testing and vaccine services for COVID-19 can open doors to cybercriminals.

Enlist Their Help

It's not enough to tell employees what *not* to do. You have to help them understand why. Show them how their actions can be compromised. This includes teaching employees to identify phishing attempts. And encourage them to pick up the phone and ask if an email request is legitimate. Let them know, for example, that they should never expect a personal request from a CEO over email. And provide examples of what suspicious emails and links look like as they happen.

For example, when an employee reports a suspicious email with a questionable link or attachment, alert other employees to the threat and call out what distinguishes it from a legitimate email. By inviting employees to play a critical role in your prevention processes, you're helping to give them a sense of ownership in protecting the company and your customers.

Intertek Alchemy provides employee training courses on all five of these areas, in addition to over a hundred other training courses specific to manufacturing workers.