IT'S TIME TO "GET SMART" ABOUT YOUR CYBERSECURITY!

TECH TIPS
By Kelly McNeil, TechBldrs, Inc.

"The human factor"— aka "the actions of employees"— plays a major role in making businesses vulnerable worldwide, whether it's from being careless with security precautions or not educating themselves. According to cybersecurity company Kaspersky, 52 percent of businesses believe that they're at significant risk from within. They believe that employees, whether through their own carelessness or lack of knowledge, put the business at risk.

And, overwhelmingly, that's shown to be true. One of the hardest-hit companies by the WannaCry ransomware epidemic last year was compromised by an employee who manually disabled important security settings on their computer, which allowed the ransomware to spread across the entire corporate network.

So why do people choose to be stupid with security? And what can you do to stop the damage "the human factor" can do to your cybersecurity?

What is "being stupid" with your cybersecurity?

Stupidity is knowing the facts and correct information, and disregarding them — hence the adage "you can't fix stupid." Stupidity is also someone watching important security updates slip by because they hear about ransomware and hacking happening at large, multi-national companies and think "well, that won't happen to me!" We wish we could tell everyone how wrong they were!

And the number one reason why people disregard their security? Convenience. Even if you know you shouldn't have the same password for all of your accounts, or that you shouldn't ignore Windows and program updates and take time to apply them and reboot, it's easier. This is the exact thought process that hackers exploit daily to infect computers around the world. Malicious actors count on the fact that people want things to be simple for them, are too lazy to keep up with important computer and security updates, or simply don't have the relevant knowledge to take informed action.

How can I be smart with my cybersecurity, instead?

In some ways, trying to convince people to take cybersecurity seriously is like teaching your kids about "stranger danger." The concept that other people are out to get you is scary, but by knowing about the danger beforehand you can keep yourself, your information, and your company safe. And it's important that you're vigilant *before* disaster strikes, not after (it won't help you then!).

The more educated your employees are about cybersecurity, the more likely they are to take precautions seriously. In our experience at TechBldrs, we've found that employee training in cybersecurity and raising awareness of security issues is essential towards motivating them to pay attention to security threats and the appropriate countermeasures. Installing updates, knowing how to recognize a spam email, and creating secure personal passwords shouldn't always be on the "I'll get around to it later" portion of an employee's to-do list!

TECH TIPS
(Continued from page 46)

In short: training and awareness are the only two ways to keep the stupidity at bay!

Businesses face a cybersecurity threat from within in the form of their employees on a daily basis. Being careless or "stupid" with your technology and security can cost you and your company money, time, and the trust of clients and employees.

It's time to get smart! If you'd like to make sure your employees can arm themselves with the tips, tricks, and knowledge they need to protect themselves against the cyber threats that are targeting them, call TechBldrs at 610.601.8017 to discuss setting up a cybersecurity training session for your company.

Still have questions? Check out our blog for more cybersecurity information at www.TechBldrs.com/blog! We also recommend reading Kaspersky Daily and Naked Security by Sophos to keep yourself aware of the latest cybersecurity news.