Busting the Most Common Cybersecurity Myths – Part Two

Viruses are Easy to Detect

When someone thinks of a computer virus, what usually comes to mind? Maybe a computer that becomes overrun with popups that appear faster than they can be closed. Or maybe a virus that crashes your computer or locks you out of your own account; holding your operating system hostage until you fork over some form of personal information. The reality is that malware has been getting more devious over the years. Now, viruses can quietly sit within your system without detection. Some can lie in wait until activated by a Twitter meme, wherein it will then take screenshots of your login credentials and send those images back to a hacker. Others have been combined with the newest AI technology to lie dormant inside phony software until activated by a specific audio cue, location, or facial recognition hit. Malware has also moved on to infect phones through seemingly legitimate (and benign) photo and fashion apps. The organizations behind these malware-ridden downloads often publish two of the exact same app; one is legitimate and the other is a virus. The legitimate app with often rank in top charts or trending categories, but when users search for it, they have a 50-50 chance of downloading the harmful version.

What can you do to prevent falling victim to online aggressors? Always check the legitimacy of anything you download. Earlier this year Mac users were targeted by a phony Adobe Flash update, hitting 190,000 users in a two-day span in January. It fooled users with a legitimate-looking pop-up, but directed them to a website with an incredibly suspicious URL. This could have been avoided if those users had simply checked where they were downloading an “update” from. You can also help prevent viruses by keeping your operating system and/or antivirus software up-to-date, as companies are constantly working to stay ahead of these cyberthreats. If you’re worried about your phone, double-check every app you download. You can also keep track of any data usage; a huge spike by one app could signal malware and should be deleted right away.

Cyberattacks Only Happen Externally

External cyberattacks are absolutely an issue in our exceedingly online-based world. Individual criminals and state-sponsored hackers are always looking for new ways to destroy or steal information on a personal, corporate, or governmental level. For example, WannaCry Ransomware, which we talked about previously in this series, was eventually discovered to have been orchestrated by the North Korean government. These Big Bad external forces are often what people focus on, as they’re what we see in movies, tv shows, and in the media when a government or big corporation is targeted. However, particularly for small or medium-sized businesses, the more pressing threat of cyberattacks are from internal sources.

Research shows up to 75% of cyberthreats come from internal employees. These aggressors can come in all shapes and sizes. They could be current or former disgruntled workers out for revenge because of poor workplace treatment. They could also be perfectly happy employees without proper cybersecurity training, who accidentally mismanage their access to private information. It could even be from an outside business partner, who have themselves been the victim of a cyberattack, with access to your own collection of private information that has become compromised by proxy. These internal threats are varied and prevalent across small and medium-sized businesses, and the results can be expensive. Damages from insider incidents can cost organizations between $100,000 and $500,000 per occurrence.

So, what can you do to prevent these threats, regardless of whether they're malicious or accidental? The main focus should be on training and educating all staff on data protection and cybersecurity. A large percentage of incidents occur from simple human error, so educating every individual in your workforce can help prevent unintended data breaches. Another option is limiting and monitoring information access among employees, contractors, and business partners, as well as closing orphaned accounts. Businesses can also invest in a full-time IT department, whose job would include helping to monitor and combat threats.

Why Do I Need to Worry About Cybersecurity? I Already Have an IT Department for That

Many businesses have already been proactive in their fight against cyberthreats by staffing an IT Department, which is commendable. However, some of these same businesses make the mistake of assuming, with IT experts on-hand, their cybersecurity protections are now complete. That is simply not the case. An IT department is not the beginning and end of all cybersecurity literacy in a company. They may be the ones who work to detect and combat viruses or hackers, but every single employee in the company has a responsibility to be vigilant. Every employee must be aware of the doorways in which hackers can enter, so they can remain vigilant to ensure they're not leaving those doors open. All it takes is a single employee clicking on a spam link while on a work computer, or while on a personal device connected to the company's wifi, to compromise the entire system. The threat may not even be a spam email sent personally to an employee. Threats could come from a benign-looking URL in a Facebook friend's message, or in an email sent by a parent. Anyone outside of the company can become compromised by clicking on something they shouldn't. The malware can subsequently spread to a friend or relative within the company, and finally into the company's entire system.

With all of this in mind, you may be asking what you can do to fully protect your company. Like one of our previous points says, education is key. Increasing cybersecurity literacy among your regular, non-IT employees can help bolster the protections an IT department offers. It's also important to realize that cybersecurity is not a one and done deal. Malware changes rapidly year after year; hackers are continuously writing new programs that are both harder to detect and harder to get rid of, so work to combat their threats must also be a constant process.

Cybersecurity is Too Expensive! I'll Deal with It After the Fact

For small and medium-sized businesses, the issue can often lie between a desire to bolster cybersecurity strength and the financial capability to actually carry out that wish. Businesses that don't possess the open pockets larger corporations lay claim to often have to forgo or cut back on essential areas to stay on financial track. Dedicated IT specialists or company-wide cybersecurity training is often what ends up on the chopping block. This is, unfortunately, a costly mistake. Look no further than the city of Baltimore. Earlier this year, they were the victims of a cyberattack, with hackers holding their data hostage and demanding over $70,000 in ransom payment. The mayor refused, and the city has since spent $4.6 million in an effort to recover their information, with plans to spend another $5.4 million by the end of the year. The attack was innocently and accidentally started by an employee clicking on a URL in a spam email. This simple mistake, which will ultimately cost the city of Baltimore $10 million, could have been avoided entirely if they had spent a fraction of that amount on cybersecurity employee training. Considering cyberattacks like this, and many others, have cost businesses millions upon millions of dollars, the trade off in preventative investment is worth it.

At the end of the day, the question is not IF you will become the victim of a cyberattack, but WHEN. Take the initiative to protect yourself, your employees, and your business by putting the time and effort into cybersecurity. Don't make the same mistakes so many have already made.

Did you enjoy our breakdown of the 8 most common cybersecurity myths? If you've found this article useful or would like to learn more about IT, technology, apps or software development, check out our other articles or subscribe to our newsletter.