HACKER ALERT!

DID YOU KNOW?

Hackers are also accessing your info through things like cars, refrigerators, Bluetooth mice and keyboards, WiFi routers, TVs, DVD players, Blu-ray players, radios, home security systems, nanny cams, baby monitors, and anything else with WiFi.

10 WAYS TO BE CYBER SMART

What the hackers wish you didn't know about keeping your Katy workplace safe, and what you can do to help prevent cyber threats from taking down your business

Written by Louis Lopez

The news reports are getting more alarming by the minute. In October, hackers were able to shut down a number of companies' websites including Twitter, Airbnb, Netflix, and Reddit, just to name a few. So how can the average business stay on top of these detrimental cyber threats and still conduct business? Here is a basic guide of some of the top cyber risks that are impacting Katy Area companies as well as businesses across the world.

1 Beware of Phone Call Scams

One of your employees answers a call from what sounds like an official tech support person from Microsoft claiming their computer has a virus or requires an upgrade. STOP RIGHT THERE! Train your employees to hang up on anyone wanting to do work on their computer remotely by phone. What happens is the computer gets locked down until a fee of $300-$500 is paid to repair their damage. Only a highly seasoned IT professional will be able to undo this damage and the cost is usually substantial.

2 Watch for Cryptoware Viruses

You see an alarming ransom message on your computer desktop after opening an attachment, prompting you to pay for virus protection. STOP! Immediately unplug your machine and disconnect the company server at once. Chances are your computer is infected. If you react to their ransom demands, you will be negotiating with cyber terrorists and that is never a good idea. Get immediate professional help from an IT expert who is well-trained in virus removal. These viruses invade company computers through email attachments, USB memory sticks, flash drives, infected websites, bad links, and more.

3 Educate Employees

One of the most effective ways to reduce cyber threats is to teach employees not to open bad email attachments and not to click on strange links. Emails that appear to be from credible sources often have email attachments that infect your machine. These attachments can be very tempting to

open because they can look exactly like emails sent from their own bank. Train employees to look at the URL address and to delete emails from unknown recipients immediately.

Be Malware Savvy

Like a virus, Malware causes your computer to repeat an incessant phrase like, "your computer is infected" over and over, sometimes followed by a prompt "click here to clean for $50." But wait, there's a catch. If you pay the $50, you'll definitely risk compromising the credit card used and another ransom cycle begins. Don't pay the infection to clean the infection. If you pay an IT firm instead, they will charge you to remove the infection off your computer, so either way you will have to pay. An easy solution is to use a cleaner like Malwarebytes to clean up this infection, but if you don't know how to do this, bring in an IT expert.

Surf the Web Safely

When employees surf the web, a simple misspelling of a well-known website can lead them to being redirected to other, more harmful websites. The bad guys get paid referral fees from sites trying to generate web traffic so they find sneaky ways to redirect as many web browsers as possible to sites web surfers don't want to visit. From there, your computer is now re-engineered to take you to a site, or a list of sites, created by this referrer. Malwarebytes will usually work well to help resolve this issue.

Don't Allow Screensaver Downloads

Employees love free screen savers with pretty images they can look at during their work day. This seems harmless, but screensaver downloads are often bundled with malware and viruses. After downloading your pretty screen saver, your computer is now flooded with overlay videos, audio files, and ad pop-ups that never go away. Malwarebytes can likely clean this up as well, but it's better not to allow them in the first place.

Forbid Free Software Downloads

Similar to the screensaver scam, free software is often bundled with viruses and malware galore. But how do you tell the good ones from the bad? Most employees won't know the difference so it's important set a policy that they need to get approval from your IT department.

Perform Computer and OS Updates

Regular computer updates are needed because they are designed to prevent the latest malicious cyber threats from invading your computer. By not installing them right away, your company is at risk for viruses. The irony is that sometimes when you perform updates, a computer may malfunction as a result of the update. Although this happens quite often, there is not much businesses can do about it. Regular updating has become an acceptable risk to ward off new and harmful viruses.

Don't Go Phishing

Responding to an official looking email from the IRS or accidentally typing a website address incorrectly can make your employee the victim of a phishing scams. Here's how it works: An employee thinks he's typed chase.com in the browser bar, but actually he typed chasee.com (with an extra e). Now he is being redirected to a Chase bank look-alike website. The employee logs in as usual, only this time he's just entered his banking credentials on a Russian website, www.chase.com-account.ru, and they now have his Chase bank login and access to his account. Train all employees to pay close attention to the URL address bar which should have an https:// prefix (for secures websites) and match the website name that was intended.

Use Unique Passwords for all Accounts

A major way hackers access your business is through weak passwords that can be pretty easily hacked. Train your employees to use more complex, unique passwords for every account. Experts recommend padding your password with five extra characters because it drastically reduces your hacker risk for being hacked. For example: Chicken57!..... (with a capital letter, exclamation point, and five periods) is much less risky than chicken57.

TRAINING CYBER SMART EMPLOYEES

Have a strong IT policy in place and make sure your employees are trained to follow these cyber safe guidelines in the workplace.

Keep Machines Clean
Have clear rules for what employees can and cannot download on their work computers. Also, keep their machines updated.

Have Strong Passwords
Make them at least 12 characters long and create unique passwords for every account.

Don't Open Attachments
Teach employees how to refrain from opening suspicious links in emails, online ads, messages or attachments.

Report Anything Questionable
If they suspect something is wrong with their computer, train them to notify the IT department immediately.

LOUIS LOPEZ is a Katy-based IT expert with more than 130 certifications. He is the owner of MILE Technologies.