E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

January 2018

In this issue…

Data safety: The non-technical way

Keeping up with advancements in technology as a business owner is tough, especially when those advancements relate to information security. However, it doesn't have to be. Here are a few physical security tips you can implement to protect your data before calling us!

Cover up your webcam

There must be some credibility to doing this if Facebook founder, Mark Zuckerberg, former FBI director, James Comey, and NSA whistleblower Edward Snowden all believe their webcams could be compromised. This is not just another paranoid celebrity reaction to ruthless paparazzi, there's a genuine reason behind it. Kindly take a moment to consider the following scenario: hackers using your webcam to spy on you. Though it might sound unrealistic, this actually happened on several occasions. Sometimes for purely voyeuristic reasons and sometimes what appeared to be espionage. This is a very real threat with disturbing repercussions. Hackers aim to gain personal information based on your surroundings, deduce your location, as well as spy on the people you're with, ultimately using this information to hold you ransom, threatening to broadcast your most intimate and vulnerable moments if you don't pay up.

Fortunately, guarding yourself against such danger is really easy and some painter's tape over your webcam should do the trick. If you're not confident about regular tape, you can purchase a cheap webcam cover online or at any hardware store.

Purchase a privacy shield

Think of privacy guards as those iPhone scratch protectors, but with an anti-snooping feature. These are thin covers you put on your computer, laptop or smartphone screen to limit viewing angles. Once installed, anyone trying to look at your screen from anywhere -- except straight-on -- sees nothing. Privacy filters are commonly used to protect work devices, particularly which display or contain critical files with sensitive data or confidential information. However, less sensitive, personal devices are still vulnerable to 'shoulder surfing' -- the act of peeking at someone else's screen, with or without ill intent, which is why we recommend using these protectors on all your devices.

Use a physical authentication key

Requiring more than one set of credentials to access sensitive resources is common sense, and has become standard practice for established online services. With something called two-factor authentication in place, you gain access to your account only after you've entered the authentication code, which the website sends to your smartphone once you've entered your account credentials. Until recently, two-factor authentication relied mostly on text messages that were sent to mobile phones. But professionals have now realised that phones can be hijacked to redirect text messages.

Moreover, authentication codes can be stolen, or users can be tricked into entering these codes via a convincing phishing website. If you're looking for authentication services that cannot be hijacked, stolen or lost, your best bet is a USB or Bluetooth key you can carry on your keychain. This means nobody -- not even you -- will be able to access your account without the physical key. Ultimate security at your fingertips.

Is your browser safe from Spectre?

The Chrome, Safari, Microsoft Edge, and Firefox browsers may not be as safe as you think. Security researchers recently discovered that computer chips manufactured in the past two decades contain major security vulnerabilities. One can be used by hackers to gain access to sensitive data. Read on to learn more.

What is Spectre?

To understand this unprecedented vulnerability, you need to know some computer chip basics. Modern chips try to speed up their work by storing information related to predictable and repetitive processes. Whenever CPUs perform calculations ahead of time that end up being unnecessary, the data is thrown away into a supposedly secure storage cache.

Hackers can gain access to the discarded data by using malware to create digital backdoors. From there, they can simply sneak in, sift through the private information, and even trick the processor into throwing away even more sensitive information. This is known as a Spectre attack.

Though the exploit is highly technical and difficult to execute, researchers said Spectre affects all modern processors, including those developed by Intel, AMD, and ARM.

How does it affect browsers?

As mentioned, hackers would need to install malware on a device to perform a Spectre attack. One tactic experts found effective is if hackers build a malicious program and embed it on a website. Should anyone visit the rogue website, their browser will automatically run the malicious program.

Once inside, the attacker can use Spectre to gain full access to key-strokes, encryption keys, and login credentials.

So far, there is no evidence of Spectre attacks actively being used to steal data from web browsers, but they are difficult to detect. Experts also predict hackers will likely develop specialized malware now that this information is available to the public.

Is there a way to protect myself?

Fortunately, major browser developers were quick to release updates as soon as the Spectre attack was discovered.

Mozilla also has security features to prevent some Spectre attacks, but announced a full-blown solution is in the works.

As for Chrome, users can expect an update as early as January 23. But for the time being Google recommends enabling the Site Isolation feature, which limits how much access browser plugins have to your computer. This feature can be enabled by going to your address bar and entering: chrome://flags/#enable-site-per-process.

Even though the updates may affect browser performance, it's a small price to pay compared with having your credit card or social security number stolen.
Like it or not, Spectre is just one of the many threats targeting your web browsers. That's why you should call us today. We offer expert advice and cutting-edge solutions to make sure your browsing experience is a pleasant and safe one.

MARCH MADNESS 2018!!!

It's officially 2018 and March is right around the corner! E-Safe Technologies is excited to announce the official date for our annual March Madness Event:

Thursday, March 29th

8:00am – 4:00pm

Highmark Stadium, Station Square, Pittsburgh, PA.

Be sure to register and join us for the largest event of the year. Please visit

http://www.e-safetech.com/marchmadness/

We look forward to seeing you there. We will be announcing participating vendors in the first weeks of February so stay tuned!

.

Virtualization vendors fix processor flaws

Everyone has been trying to make sense of recently discovered vulnerabilities that affect almost every computer in use today. All you really need to know about the Spectre and Meltdown bugs is that they make it very easy to spy on private information stored on a computer. But if you're using virtual desktops or servers, you're probably safe.

What are the risks of an unpatched computer?

Regardless of whether you are using a computer with all its hardware sitting on your desk, or you're connected to a virtual computer drawing most of its computing resources coming from a cloud server, you'll be using something called a central processing unit (CPU).

As unbelievably efficient pieces of technology, CPUs have been programed to recognize patterns. When a CPU recognizes a pattern, it stores everything it needs to complete that task in a temporary place. If the pattern changes, the information is thrown out. Spectre and Meltdown allow hackers to not only view trashed patterns, but also to trick a CPU into thinking a specific pattern has changed and should be dumped into this vulnerable storage.

In worst case scenarios, this could affect credit card information, passwords, and personally identifiable information. And even though a virtual desktop or server is created with software that partitions hardware resources on a large computer into several smaller, standalone computers -- Spectre and Meltdown flaws are still present

Spectre and Meltdown flaws are still present.

The Chrome, Safari, Microsoft Edge, and Firefox browsers may not be as safe as you think. Security researchers recently discovered that computer chips manufactured in the past two decades contain major security vulnerabilities. One can be used by hackers to gain access to sensitive data. Read on to learn more.

How are they fixed?

Because these are hardware-level vulnerabilities, the only way to truly fix them is by replacing the CPUs. But because there aren't any processors currently available without the Spectre and Meltdown flaws, software patches are the only option.

Amazon Web Services, Microsoft, and Google have all installed updates that essentially tell CPUs to stop recognizing patterns to store data ahead of time. However, predictive functions significantly increased the computing speeds of modern computers, meaning turning them off will slow down computer performance.

Virtualization is more cost effective than ever

This all sounds terrible, but it's actually a huge selling point for virtual desktops and servers. First, it proves that big-name cloud platforms can push out urgent security updates to thousands upon thousands of clients in a relatively quick fashion. Those using "traditional" computers (remember, the ones with all the hardware sitting on your desk), need to apply these patches one-by-one, on-site.

Second, most virtualization platforms charge on a pay-for-what-you-use model. So, you're not paying for hardware and its flaws, you're paying for the actual work that is finished on your web-accessible computer.

Spectre and Meltdown will continue to affect the computing world for several months to come. However, businesses that use virtualization technology will not be hit nearly as hard. There's no better time to make the switch than now -- give us a call today.