THE NAVIGATOR
COMPASS
NETWORK GROUP

JANUARY 2016

In this issue...

The hack you never saw coming

GlebStock / Shutterstock.com

Once upon a time, browsing the internet and avoiding malware was a relatively simple task. All you really had to do was be on the lookout for sketchy websites. And even then, when you did land on a sketchy one, you would only panic for the half-second it took for you to click the back button. After that, your blood pressure would teeter back off to normal levels and all would be right with the world.

Until now.

Introducing Malvertising—the malware that poses as a legitimate ad and can affect your computer with no clicking or downloading necessary. This nasty form of malware can be found on any website (not just the sketchy ones). In fact, in 2015, many popular websites were unwitting hosts to Malvertising—including sites like Yahoo, Reuters, The Daily Mail, Perez Hilton, CBS Sports, Yahoo, and eBay.

If you're not panicking yet, then just wait.

What makes Malvertising so vicious is that it can infect your computer with no action on your end. All you have to do is visit the host site. So, in theory, if you visited the UK website, Daily Mail, in October of last year when they were infected with Malvertising, you may have been subjected to a drive-by download, which exploits outdated software or apps to infect your system with a virus. If you had actually clicked on the ad, you would have been exposed to an unpleasant form of ransomware called the Angler Exploit Kit.

According to Wired Magazine, Malvertising is considered a "sweet spot" for many cyber criminals because it yields great returns and is almost entirely anonymous. It yields great returns because it is a direct line of attack that most people won't be able to recognize, and it is almost entirely anonymous because the ads rotate quickly and can be purchased through illegitimate means such as stolen credit card information (which means it's nearly impossible to trace).

Now the question you should be asking yourself right now is how do I avoid Malvertising? And you may not like the answer. You see, the only way to proactively avoid this form of malware is to always keep your system up-to-date—this includes your anti-virus, as well (something you should already be doing) and this requires you to work a little.

If you don't allow automatic updates to your browser, operating system, or security solution, then you need to make sure you proactively seek out updates on a continual basis. Think of it this way: Updates make your system whole. When you miss or postpone critical updates, you create holes in your system that grow bigger each day. These holes serve as entry points for hackers and cyber criminals.

Sources

https://blogs.mcafee.com/consumer/drive-by-download/

http://www.bbc.com/news/technology-34541915

https://nakedsecurity.sophos.com/2015/10/19/malvertising-meets-the-daily-mail/

http://www.cio.com/article/2948133/malware/malvertising-reaches-record-levels-in-june.html

http://www.wired.com/insights/2014/11/malvertising-is-cybercriminals-latest-sweet-spot/

Monkey Business Images / Shutterstock.com

4 tips to keep your children safe online.

The Internet of Things has expanded more than most people ever imagined it could. People are constantly connected to things, and things are indefinitely connected to other things. This concept has had a significant impact on the way our children are brought up. Younger generations have trouble even differentiating between 'online' and 'offline'—they're simply 'online' at all times. There is no such thing as 'offline' to younger generations.

Men, Women, and Children, a movie released earlier this year, centers on young adults and children growing up in an online world. The movie heavily focuses on how parents struggle to deal with it on a daily basis, never knowing where to draw the line or how to do it. And this probably rings true for many real-life parents. How do I teach my children online safety? What is acceptable for them to do? What should they not be doing? How do I guide them in the right direction without overstepping?

There are many different ways to lead your children down a secure path, and there are a few good organizations out there that present useful 'how-to' material such as ikeepsafe and NetSmartz. But here are a few tips to help you get started.

Start at the very beginning.

Parenting.com compares your child's online world to a playground. You know who your child is playing with, and you know all about the park they're playing at. So why wouldn't you do the same with their 'online playground'? They're big advocates of copiloting—sitting with your child and being in the same online playground as they are. But don't take this the wrong way.

This doesn't mean sitting with your 15-year old or even your 10-year old. This means starting from the very beginning when your young child is barely learning how to navigate connected devices.

Teach them what is right and what is wrong.

You can't assume your children know what is right and what is wrong online. How do you expect them to stay safe online if you've never told them how to be safe? As technology changes and as your children get older, you should have multiple conversations with them about what you believe to be acceptable and not acceptable. Give them clear, understandable guidelines. For example, do not share your physical address with anyone online. But don't just leave at that. Explain why they cannot share their information and what the consequences may be.

Enable parental controls.

Parental controls are necessary. And depending on your children, you can make the decision as to how long they're necessary and to what degree they're needed. Most all devices—tablets, phones, computers, TVs—all have parental control settings or downloadable applications that are easy to navigate and even easier to implement. Here's a great video from O2 Guru, a UK-based digital communications company, on how to find these settings and applications.

Explain the meaning behind online reputation.

Many times, online reputation is used within a business context; however, it can also be used to describe an individual's collection of online material. There are companies that make a living off of protecting and preserving your online reputation, the inherent masters of Online Reputation Management. You need to explain to your children why these companies exist, and how people find their way to these companies. They need to understand that their online actions today can haunt them 10, 20, or even 30 years from now, ruining job prospects and personal relationships.

5 honorary mentions from the strange history of tech

PC World compiled a list of 14 "strange but true facts" that hold a place in the history of technology. Here are some honorary mentions:

Amazon was originally named Cadabra, but was later changed because it sounded too much like cadaver. The name "Amazon" was chosen in part because of Yahoo's search engine ranking, which, at the time, ranked sites alphabetically.

Nintendo didn't start off in technology. They were in the playing card industry for 67 years. It wasn't until a visit to the US in 1956 that the owner decided to branch out.

In Nigeria, Ghana, and Bangladesh, less than 1% of all homes have a landline connection, yet 85% of all citizens have a cellphone. They completely avoided the landline era.

Ever wondered what the first ever webpage looked like? Well, you don't have to wonder because it still exists to this day. It was created by Tim Berners-Lee on August 6, 1991 with regards to a project he was currently working on. Something by the name of W3 or, what some people like to call, the World Wide Web.

A Hollywood actress by the name of Hedy Lamarr and avant-garde composer, George Antheil, are considered the parents of modern-day Wi-Fi. They developed a precursor to Wi-Fi that allowed radio signals sent to torpedoes to "hop from frequency to frequency" without being jammed up in the process. It was adopted during the Cuban Missile Crisis 20 years after invention.

Everett Collection / Shutterstock.com

Does HIPAA have any influence over wearable tech?

A few years from now, most of the people you see will wear an activity tracker of some sort—on their wrist, pinned to their shirt, or attached to their sock. And if it's not a dedicated activity tracker—like a Garmin, Misfit, or Jawbone—then it will be integrated within your smartphone or watch.

Early in 2014, one out of every six people owned a piece of wearable tech, according to a survey administered by Nielsen. Out of the batch of people who did not own wearable tech at the time, half of them were interested in buying it. These people asserted that fashion and expense were the two main reasons preventing them from purchasing wearable tech.

But that will soon change. Companies like Misfit already offer wearable tech for as low as $30, as well as an upscale collection called Swarovski Shine, diamond-infused wearables that seamlessly integrate with bracelets, wristbands, and necklaces.

As of mid-2014, 68% of all activity trackers sold in America came from Fitbit, the company that claims they have a product for everyone. So why is this important? Why does it matter how many people may or may not own wearable tech or fitness trackers in the future?

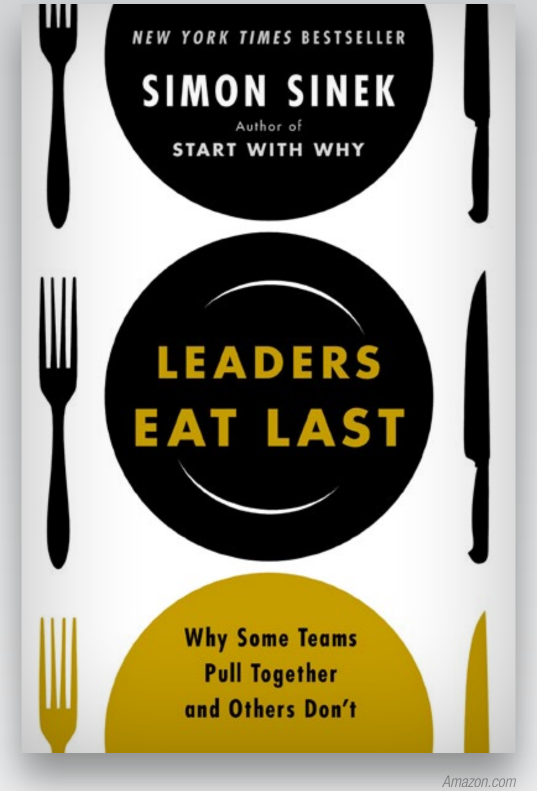
Because of HIPAA… and Fitbit is one of the first wearable producers to realize this.

From Covered Entities and Business Associates to Business Associates that are really just another extension of a Covered Entity, many companies are liable for upholding HIPAA regulations. Technically speaking, HIPAA could very well expand to cover a cleaning service, a law firm, and even an answering service.

Although HIPAA doesn't currently cover data that most activity trackers transmit—like the amount of steps you take in one day—that's not to say that one or two years from now it won't. Fitbit understands this. Recently, they took a "proactive step" and participated in a full-blown HIPAA audit. As a result, they can now actively seek out partnerships with various Covered Entities and work inside businesses in a corporate environment as compared to with consumers only.

It should be interesting to see how wearable tech fits into HIPAA jurisdictions in the future. As of right now, if you receive this technology directly from a Covered Entity such as your primary doctor, then it is covered under HIPAA. But otherwise, the fitness and health data transmitted from your tech can go wherever the manufacturer wants it to go—as long as it's included in the terms and conditions.

Geoff Goldswain / Shutterstock.com


NEW YORK TIMES BESTSELLER
SIMON SINEK
Author of
START WITH WHY
LEADERS EAT LAST
Why Some Teams Pull Together and Others Don't

Amazon.com

Book Review: Leaders Eat Last

Why is that some companies have loyal employees who love their job and everything about it? Yet, other's fail to even make their employees semi-content?

Is it because that's the job they were always meant for? Every moment in their life led up to this one job, this ultimate career. It was simply predestined.

Or is it because of the killer perks? The clients are easy to please; there's free food in the breakroom and every quarter there's a decent-sized bonus.

Simon Sinek, the author of the bestseller, Start With Why, says none of the above. In his inspirational book, Leaders Eat Last, Simon illustrates how and why some companies are simply better than others.

And it all starts with their leader.

Simon travels through real-life examples and motivational stories of leaders who lead better and by doing so, build and craft a naturally cohesive team. He explains his theory behind The Circle of Safety, a concept where teams work together to defeat a common enemy, and ties it back into human biology.

If you haven't already done so, consider picking up a copy of Leaders Eat Last and discover how to be the leader people need you to be.