POST-PRESENTATION Q & A WITH ANNE SAITA

Thanks, everyone, for providing great questions during my presentation on consumer data security. As promised, I'm responding to questions that weren't answered live and also a few that were that may require more information or a clarification.

What sites are used to post the fake new to install malware. Is it primarily Facebook etc. or can they appear on legit retail sites such as Target?

By "fake news," I was referring specifically to malicious websites and news articles that appear similar to trusted ones. They are designed to spread malware by appearing to be from a news organization. And, yes, they may pop up in your social network feeds and online ads on a site you regularly (or rarely) use. Here's a good article that explains what's at play: https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

This is also a good read on the other type of "fake news" in which people are spreading misinformation on COVID-19, and how to spot them: https://theconversation.com/how-to-spot-coronavirus-fake-news-an-expert-guide-133843.

Can't hackers figure out that @ is a popular substitute for a in strong passwords and that zero is a popular substitute for letter O, etc.?

I answered this but wanted to emphasize that the "key" to letter/number/character swamps is up to you and the word or phrase it actually refers to you would be tough for someone else to guess and then slice and dice (no pet names, kid names, maiden names, etc.) In my original example, not all @ symbols were swapped to make the codes even stronger. Then I simplified it for the presentation so the concept was easier to ingest. If this approach is new to you, you may start with a key that's easier to remember, especially if you are locked out after 3 attempts. You can then update a password with more difficult variations once the word or phrase is internalized.

Why would it be safe to even enter a password on public WIFI?

It wouldn't, unless you are using a mechanism to scramble the data being sent over the unprotected internet, such as personal VPN. Some people set up or access what appear to be innocuous accounts while in airports, restaurants, coffee shops, waiting in public for friend, etc. Avoid doing that on an "open" wireless line whenever possible.

Is what one VPN product better than another?

I appreciated all the interest in VPNs, and promised a list of product review sites that might help determine the best solution for your needs. I reviewed several expert "best of" and these were consistently named in the top 5.

NordVPN: https://nordvpn.com/
TunnelBear (good for first-timers): https://www.tunnelbear.com/
ExpressVPN: https://www.expressvpn.com
Surfshark: https://surfshark.com
CyberGhost: https://www.cyberghostvpn.com

Pricing, features, compatibility and ease of use will help you determine which of these, as well as others, may be best for you. As mentioned during the presentation, most of these offer free trial periods and there are personal VPNs out there that are free but limited in what is offered.

Is the Microsoft Win 10 security software enough?

It's definitely better than its predecessor since it comes with anti-malware software and basic intrusion detection (i.e., firewall) by default. Depending on what you do while using that device, it may be enough.

Did you say to call the number in an email? Should never do that! Look up real number to the company on their website or on a document you have from them that you know to be legit.

Not sure about the complete prohibition, but this comment reminded me of a step I failed to mention. When you get an email that looks like it's from a trusted sender (address verified) but aren't sure, and a number is provided, copy that number in a web browser and see what turns up. Be aware that sometimes companies only list general phone numbers on their web site but provide a more specific one in an email, so you may have a valid request but it doesn't match the number online. You also can use crowdsourced sites, but contributors don't always distinguish between legitimate businesses, spammers and scammers.

I stopped using Google search a long time ago, and never adopted Google Chrome, because of their pervasive collection of data. I now use DuckDuckGo.com as my default search engine. Any ideas/comments on this?

I've heard good things about this lesser known, but increasingly more robust, search engine in terms of privacy. If it yields the results you want, you should be good. Really, any web browser can be made more secure/private by applying more rigorous settings. Thanks for bringing up alternatives to the major web browsers.

Could you discuss information aggregators like MyLife?

MyLife is among sites that gather and post publicly available information on individuals, but they also are often seen as highly invasive and often inaccurate. There's normally a fee beyond a certain number of queries or to go deeper into someone's profile. These sites need to be self-monitored and -managed on an ongoing basis. And, under CCPA you have the right now to either have incorrect information fixed or your entire entry removed from both the site and database.

Is SIM hi-jacking of your mobile phone number considered a risk with two-step verification?

Yes, it is. With SIM hijacking, someone convinces your cell phone carrier to switch SIM numbers from yours to theirs. In doing so, they now get the texts or calls with a verification code as the second factor. It's still far less common than other exploits but worth knowing, so thank you for that.

Here's a good, consumer-friendly article on how it works and what you can do:
https://www.wired.com/story/sim-swap-attack-defend-phone/

My credit score is 830, after over 10 year credit freeze. I can unlock it and specific a period for which it needs to be unlocked. It is easy for 2 of the 3 agencies.

When I first froze my credit almost 20 years ago, there weren't as many cybercrime victims and it was difficult to unfreeze an account in a timely manner—like when you are ready to purchase a house, a car, a cell phone, pay for a purchase with a credit card, etc. The last time I froze my credit, those restrictions were still in place and you also had to pay a fee each time you requested a temporary thaw per credit agency. Newer legislation now makes that free. It sounds from this question and feedback I received after my talk, that today's credit freezes, now more commonplace, do not impact current credit card use. And I'm happy that credit scores apparently are no longer being impacted. That's progress!

I shared my own personal travails to underscore a pain point that still exists if you need to unlock credit quickly from all three agencies. If you rarely need access to such credit, a freeze isn't as much of an inconvenience. Especially if you can unlock it for a short period of time and therefore reduce your exposure.

I did not want to suggest credit freezes aren't a best practice – they are. Just remember they don't protect against the credit you already have. That's where regular monitoring through the three main agencies and your credit card providers help. I check all of my financial accounts daily for any anomalies. Something tells me many of you do too.

My computer says that Microsoft is no longer supporting my operating system. What should I do?

Update to a newer operating system. Microsoft is letting you know it won't be responsible for any successful attacks launched using a security flaw in the OS discovered once it stops its support. There have been instances in the past where bug hunters found a very serious flaw on older-yet-still-widely-used OSes or software and issued a patch anyway. But don't count on it. Upgrade if and when you can.

Recommended sites:

Many of the sites I visit to keep up on cybersecurity trends are very technical. Here are some popular with both tech professionals and consumers.

Investigative Journalist Brian Krebs' blog: https://krebsonsecurity.com
Dark Reading (Attacks and Breaches section): https://www.darkreading.com/attacks-breaches.asp
Troy Hunt's Blog (creator of Have I Been Pwned?): https://www.troyhunt.com

And here are some sites I mentioned (and one I meant to) for tech product reviews:
https://www.cnet.com
https://www.zdnet.com
https://www.theverge.com/tech

Remember that there are risks with everything we do or use, and those risks may be acceptable if the value outweighs them. Nothing is 100% secure, but if we practice best practices proven to mitigate those risks, then chances are good you'll stay safe from cyber intruders and phish scammers.

If you have questions that popped up after our presentation, I'd be happy to try and answer them in the coming weeks. You can reach me at asaita@twirlingtigermedia.com.