Cybersecurity for a Changing World

While SDA EdSymposium19 offered plenty of interesting seminars with lots of useful information, there was one seminar in particular that really jolted me because the speaker scared the living daylight out of me with her straight talk. That was Heather Stratford, CEO of Stronger International, with her presentation “Phishing Trends and Cyber Attacks.”

Heather’s background is in cybersecurity, and while based in Spokane, her work has no boundaries. We’ve all read numerous news accounts of companies who were hacked due to a hole in or failure of cybersecurity, and the fallout for many thousands or millions of customers whose personal info was released. But by whom, and how did it happen in the first place?

She offered up a startling statistic. Can you guess how many “connected” devices there were in 2017? These would be phones, computers, home alarm systems, cars with Bluetooth, appliances, medical alert systems – anything that can connect to the internet. Would you believe 20.35 BILLION?! And it’s projected to increase to a staggering 30.73 billion by 2020! That’s a lot of potential hacking portals.

She reminded us of the big Target hack in 2013. While Target had relatively strong cybersecurity systems in place, one of their vendors didn’t. An HVAC provider was testing the connected thermostat with a connected handheld device, and the hackers were able to access through that portal Target customers’ personal info stored in the credit/debit card database. About 110 million Target customers increased their chances of more phishing attacks as the hackers, now armed with email addresses, sought to gain even more personal info from them. And right before the holiday shopping season . . .

Another prominent hacking event was unfortunately experienced by credit reporting company Equifax. They didn’t dot all the i’s and cross all the t’s in their cybersecurity, perhaps weighing the cost of protection versus the chances of being hacked or just ignoring the update reminders, and the hackers accessed 143 million Equifax’s customers’ credit histories including social security numbers. Offering credit monitoring services for a period of time to their customers has cost Equifax millions, as well as caused worry and anger for their anxious clients.

A third example she gave may not be as well known in the U.S. Aadhaar, India’s “Social Security” system, would seem to be pretty cyber secure since it uses biometrics (fingerprints, retinal scanning) for its billions of Indian citizens. But it too was hacked. The perpetrator was internal; an employee sold personal info to someone who was willing to pay big money for all that information. And the effects of that have been recurrent as numerous government agencies using that data have been lax in their cyber security.

As I write this, Puget Sound Business Journal reports that Premera Blue Cross will be paying $10 million in fines to 30 states for not securing patients’ data enough to protect it from a 2014 cyberattack, despite repeated internal and external warnings that its cybersecurity was insufficient. In addition to the fines, Premera will have to put specific data security measures in place, agree to
annual reviews of those practices, and provide data security reports to the Washington state attorney general’s office.¹

According to Heather, 90% of patches are to fix “vulnerabilities” or coding errors. When you get a message to update your computer’s operation system or programs, pay attention. Not doing it when they’re released can result in a virtual open window for hackers. An unbelievable 73 personal records per second are stolen by hackers. The stereotype of the young, male adult working solo to see how many systems he can crack just for the thrill of it is not the predominant crook profile. Rather, it’s sophisticated crime syndicates ignoring international boundaries who are really after your info. And contrary to popular belief, your credit card information, which is the low-hanging fruit, isn’t really worth much on the dark Web – maybe 25–50 cents per card number. The real money’s in medical history data; currently that’s worth much, much more – about $1000 per patient! While credit card numbers can be easily cancelled by the hackee, it’s almost impossible to change your medical history and physical characteristics.

How can you spot and thwart a phishing attack? Look for these signs:

1. The email request says it’s urgent that you respond quickly and with sensitive info.  
   Response: Never send your personal info, bank account info or passwords via email.
2. There’s an unexpected attachment.  
   Response: Be very cautious about opening or downloading attachments.
3. Instead of addressing you by your name, it’s a generic greeting.  
   Response: If a popup window asks you to enter private or personal info, don’t. Contact the purported “sender” directly. Get an email from your bank asking you to update your personal info? Contact the bank directly to see if that’s a legitimate request. At the least, they’ll want to know of phishing attacks in their name.
4. The grammar or spelling is poor.  
   Response: Carefully read the email to look for those spelling or grammatical errors.
5. And the links are strange.  
   Response: Hover over the links in the email to see who the sender is. It typically won’t match the sender’s email address.

Now that we know how potentially easy it can be for someone with nefarious goals to steal our personal info, here are some more Heather-recommended safety measures.

1. Patches – do them when they’re released. Yes, some may mess up other programs on your computer, but those are a lot easier to fix than your hacked medical or credit history.
2. Multi-factor authentication – after your initial login, a secondary security measure that requires you to enter a temporary code sent to your email account or mobile phone before you are able to access your files.
3. Password management  
   a. Longer is better, and an alphanumeric mix with spaces, symbols and a combination of upper-case and lower-case characters is even better.
   b. Random passwords are the strongest.
   c. Don’t use “personal” or obvious words. Anyone ever use “password” as their password? Any related to your family/hobby/job that can trace back to you, like “MotherOfFraidyCat” or “World’sGreatestQuilter” or “DLRGroupNewformaNinja”, are unwise.

¹ Megan Campbell, “Premera fined $10M in settlement for 2014 cyberattack” (2019 July 11), Puget Sound Business Journal
d. Don’t use the same password on multiple sites. At a bare minimum, have 3 separate passwords – one for work, one for home, and one for banking – the last one being stored somewhere very safe.

e. Don’t share your passwords, and change them regularly.

f. Use a password manager like LastPass, Dashlane, or many others that are available on the internet that can be pretty cost-effective ways to store all your passwords in one program, so you don’t have to remember all of them. Just don’t forget your master password for the password management program, or you’ll never be able to get to your stored passwords. Definitely store that master password somewhere very safe.

4. Use a VPN (virtual private network) for work when using public Wi-Fi. You can also set one up for your personal work. A VPN provides a dedicated, encrypted pathway to access the internet or your work server files without being hackable.

5. If you’re using public Wi-Fi, like you’re waiting for your flight at the airport and decide to plug your phone or laptop into a charging port, be sure to only use a power plug and outlet, not a USB port. They’re notorious pathways for malware to be installed on your phone or computer.

6. Also, when using a public Wi-Fi network, a best practice is to never access sites with financial info, like your bank account, 401k, etc.

7. What about backups? Backups of your work data should be done at least daily, and for storage providers, Lifelock and Carbonite are a couple of recommended choices. Personal records backups can be less frequent.

Ransomware attacks, where your files are locked down until you pay the perpetrator, can be scary events. If you get that black screen with an ominous ransom message, don’t shut down your computer. Disconnect from the internet, and contact your IT department or consultant.

Think all of this is too much trouble? Consider that small businesses that are hacked run a very good chance of being out of business within six months. They just never recover from the loss of data or the public relations cost of reassuring skittish clients and consultants, not to mention any financial costs of credit monitoring services or fines they offer those affected.

In the end, I left Heather’s seminar with an upside-the-head wake-up call, but also feeling well-armed with an array of tips to protect my personal and professional data.

Shannon Soady, CDFA
Senior Associate
DLR Group
Seattle, WA

The contents of SDA’s In the Know articles are considered the opinion of the author. SDA does not endorse any products or services mentioned, and SDA does not assume responsibility for any circumstance arising out of the interpretation, application, use or misuse of any information presented. SDA recommends the reader consult the appropriate legal, financial, or human resource counsel before implementing information contained herein.