About These Worksheets

Let me be the first to tell you *Congratulations!* By downloading these worksheets and consciously making the decision to go through them, you've also made the decision to improve your security.

Cybersecurity is not a spectator sport. You need to get in the game to learn more about it. That is exactly where these worksheets come in! No, you won't become a world-class hacker after going through them. However, you will gain knowledge and have a few extra tools at your disposal to better equip yourself in the digital age. Some of these exercises may surprise you at how easy they are. Fantastic! Some of these tools might terrify you. Even better! They are meant to open your eyes and help guide you on your journey to becoming more cybersecure.

Keep in mind that these worksheets are not one-and-done exercises. As mentioned several times during the training, cybercriminals are *constantly* evolving. Similarly, you need to make improvements too. Am I suggesting that you mark a date on your calendar and go through the training and worksheets every year? Well, I'll let you be the judge! ;-)

There is no better advocate for protecting your data than you!

Stay safe, healthy, and secure,

Dallas Haselhorst
Founder & Principal Consultant at TreeTop Security
GSE #231, CISSP, SANS/GIAC(x10)

Worksheet #1 - Your Data, Your Backups

Take a moment to think about what data is important to you or your business. Said another way, if you experienced a ransomware attack, natural disaster, or hard drive failure tomorrow, what would make you sick to your stomach knowing you lost it forever? Don't be afraid to take a few minutes to *really* think about it. There's a good chance your answer includes pictures, videos, documents, tax-related information, customer information, QuickBooks files, etc.

I've personally been on the winning end of data recoveries where a business thought they had lost years of customer data or when a spouse cries tears of joy after recovering pictures from her husband's last military deployment. Unfortunately, I've also been on the losing end where a mother lost all of her child's photos from birth to 5 years old. Take control… Don't let your memories and important information get left to chance. There's no better time than NOW to go back and ensure your important data is backed up appropriately. At a minimum, we recommend the 3-2-1 backup strategy (infographic below). This strategy/rule means you have 3 copies of your data, you store that data on 2 separate storage media, and one of the storage locations is off-site.

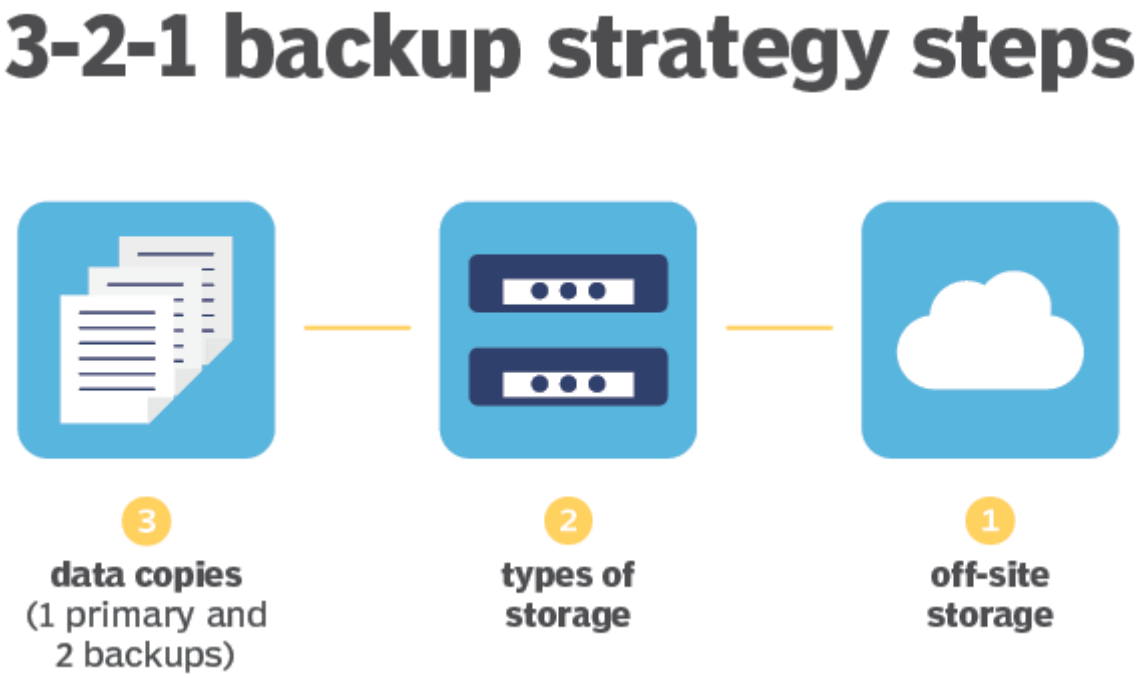


Image courtesy of TechTarget

And yes, this rule works for both home and business data. While there are ways to do backups entirely for free, we often remind customers that “free” has *costs* such as requiring human intervention. A prime example of this is inserting a USB thumb drive and asking someone to remember to run the backup, remove it from the computer, and then take it off-site or store it in the safe every night. What happens if you get busy, go on vacation, or the person responsible for backups leaves the company? The good news is that there are numerous vendors who provide backup services inexpensively. Scared about storing your data in the cloud? Well, you should! Be on the lookout for vendors who promote a zero trust or trust no one approach. What that means is your data is encrypted before it ever hits their servers, i.e. if they have a data breach, it doesn’t mean your data is exposed for all the world to see. If you are a larger business, you should really consider finding a trusted advisor to help you in designing a comprehensive solution. Contrary to popular belief, backups don’t have to be expensive to provide solid coverage and security!

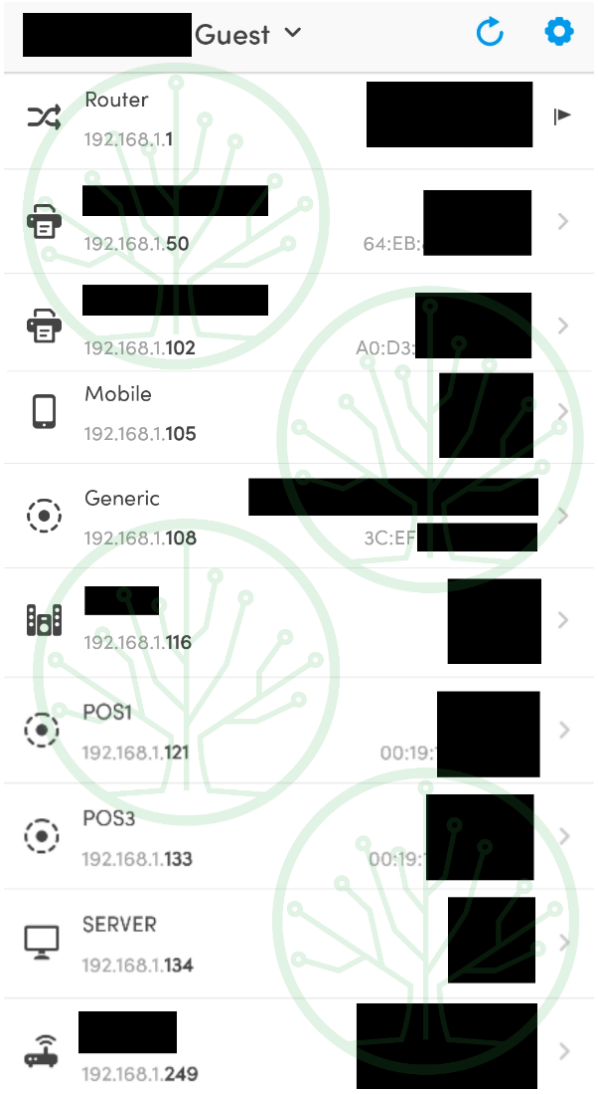
Don’t forget...

A backup by itself is only half the battle. Quite literally, your backups and data are only as good as what you can restore. If you already have a backup, you must be 100% certain you can recover from the backup. How often do you perform a test on your recovery capabilities? Have you tried recovering from a separate computer? As important, is all of the data that you “think” is included in the backup actually there? From our experience, that last one is a real sticking point where someone assumes their data is getting backed up and they only realize it isn’t when it’s too late. It’s never a bad idea to add a calendar entry as a reminder to periodically perform a backup and recovery test. At a minimum, a quarterly “restore test” is recommended.

Last but not least, never assume someone else is taking care of your data. If you have an IT department or IT provider, you’re not out-of-line for discussing backups and recovery with them. *It’s far better to have that conversation now than when it is needed.* Better yet, test out their services... Without tipping them off, move a file somewhere and then tell them you accidentally deleted it. If they can’t recover the file, then it might be time for a policy change or to consider alternative backup solutions.

Worksheet #2 - What's on your network?

Did you know that a single compromised device on your network can lead to your device getting compromised? Does that change your thoughts on potential security issues when working from home? The average home network often has a poor wi-fi password, a password that likely has never been changed, and good chance everyone and their dog has access to the network. Who has accessed your wi-fi network in the past -- your kids, neighbor kids, your friends, or maybe even relatives like long lost Aunt Sally who visited 3 years ago?



To make matters worse, there are also a LOT of devices we tend to forget about. Your task for this worksheet is 2-fold. First, think about changing your password if you haven't done so in a while and/or if your password is under 12 characters. Now, think about what devices are on your network and do a mental count of them. STOP HERE and really think about it! Write them down if you need to.

If you plan to run this application at your office, you must receive written approval from someone who has the authority to approve it. You're not quite "hacking" at this point, but some of the activity may appear as such. You've been warned!

Using your Apple or Android smartphone, download the fing app. Make sure you see the icon/name as shown above as there are look-alikes. Fing is a free app that allows us to scan the local network and see what other devices are on it. Once the app is installed and you verify you are connected to wi-fi, then simply open the app and click 'Scan for devices.' Within a

few seconds, you should start seeing results. If it's a small network, it might even be completely done scanning in under 15 seconds.

Now, take a peek at the results and scroll down if necessary. How close were you to your original estimate? Are there any devices that you completely spaced off? If you missed a few, don't worry, you are not alone. In our unscientific tests, most estimates are off by at least 25%. So whether you forgot the kids' gaming system, the doorbell, your speakers, light bulbs, the garage door, someone's tablet, your printer downstairs, your thermostat, your smart TVs, your surveillance cameras, or anything else… Rest assured, there are a lot of devices that can be overlooked!

For smaller business networks, it's pretty common for us to use fing or similar tools to get a quick lay of the land. In fact, the picture included in this section is the output of a "guest network" at a friend's restaurant business. The story goes that the owner didn't think they needed security since they were PCI compliant. <Yes, there's a joke in that comment.> Instead, the business was experiencing wireless issues and asked if that was something I could help with, i.e. not security-related (just yet). I asked for their permission to look at a few things and run a few tests. They walked away to run my credit card and I had the results from that particular picture by the time they returned with my card. Imagine their surprise [and my own being completely honest] when learning that by simply accessing the guest wi-fi, I was able to see everything on the "private" network -- other guest devices, point-of-sale terminals, servers, stereo equipment, printers, video surveillance equipment, etc. Their IT company had created a guest wi-fi connection and then proceeded to associate the guest wi-fi with their private network, i.e. guest devices/users ended up on the exact same network as their business. Yikes!

That completely defeats the purpose of setting up a guest network. Refer back to the very first comment in this section if you don't understand the significance of this finding. Long story short is that with a little bit of effort, a bad guy could have gained access to credit card data. Even worse, someone could even have deployed ransomware to lock them out of their systems!

That's the end of that story and worksheet, but this is worth mentioning since it is somewhat related. Poor configurations such as this is why a common security recommendation is to never use public wi-fi. In this case, an attacker could have targeted any guest device just as easily as the business devices. While some public hotspots are configured properly, the overwhelming majority are not. Even if they are configured correctly, there are other attacks the bad guys can use to gain access to your system.

Worksheet #3 - Password Managers & 2FA

Password Manager

Aside from the general knowledge gained with our cybersecurity awareness training, the other biggest attendee takeaway is the need to implement a password manager. How do we know that? Because we constantly receive emails or hear things like “thanks for talking me into that” or “I didn’t know it would be that easy.” And that’s fantastic because a password manager is an absolute must for your security! It’s worth mentioning that there are a lot of password managers on the market. If you currently use one and you like it, then skip ahead to the 2-factor authentication section in this same worksheet.

If you need a little more of a nudge to implement a password manager, then this guide is for you because we are going to walk through the high points of the process using the excellent free service, Bitwarden. If you are a business/enterprise, Bitwarden does also offer paid services that allow you to share passwords between team members. They even have a family plan that allows you to share login data with other family members.

First, go to the website below, fill in the information, and then click submit. Follow the advice from the TreeTop cybersecurity awareness training and use a long, 20+ character passphrase for your master password. This should go without saying, but don’t forget it!!!
https://vault.bitwarden.com/#/register

From there, go to the Vault page and login. You will receive a verification email.
https://vault.bitwarden.com/#/

Once you have Bitwarden setup, go to a website, type in your username and password, and Bitwarden *should* ask you if you want to store the information in the vault. The “manual interaction” lessens over time once you use it for a while. Although it is outside of the scope of this tutorial, if you have an existing spreadsheet of usernames/passwords, you can import that data into Bitwarden. You can even export data from other password managers and import them into Bitwarden. Bitwarden also has an app for your mobile devices whether Android or Apple-based, which means you can synchronize your passwords across all devices!

2-Factor Authentication (2FA)

As we discussed in the awareness training, 2-factor authentication (2FA) is a HUGE boost to security. An extremely common tactic cybercriminals use is to send a phishing email and then direct you to a fake login web page to “capture” your username/password. Once they get your account credentials, they can then login as you to access documents or other information. If they gain access to your email account, they could scam your friends, family, or business associates on your behalf. Better yet, they could use your email address to reset your other accounts! Think about it… If you go to a website and click “Forgot password” where does that password reset go? We strongly encourage some form of 2FA on every email account as well as accounts that need a higher level of security.

From the CNET website, here are instructions on how to enable 2FA for some popular websites and/or services (link below). Keep in mind that this is not an exhaustive list. Most websites and services now offer some aspect of 2FA. If it’s offered, you will usually find it in the same area as your profile settings after you login. If you can’t find it, reach out to the company in question to ask where it is. If they don’t offer it, ask them why not! ;-)

https://www.cnet.com/how-to/how-and-why-to-use-two-factor-authentication/

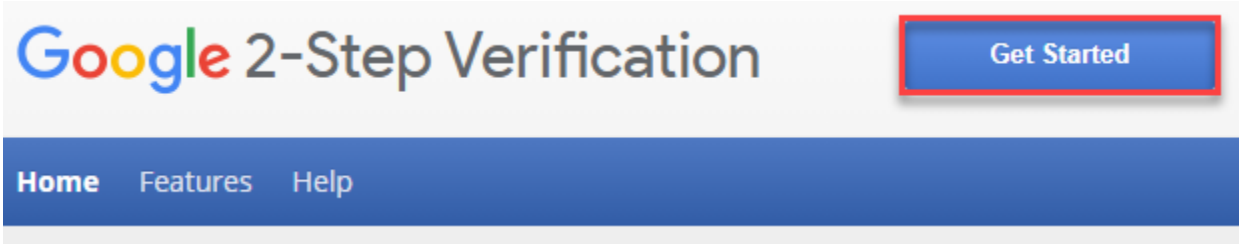
Amazon
Sign in to your Amazon account, click Account & Lists at the top right and then go to Your Account > Login & Security Settings and click the Edit button for Advanced Security Settings. Click the yellow Get Started button and sign up to receive codes via SMS or an authenticator app. You'll also need to add a backup phone number to lessen the odds of getting locked out of your account. For more, see this Amazon help page.

Apple
From an iOS device, go to Settings > iCloud, sign in if you aren't already and then tap on your Apple ID. From your Apple ID page, tap Password & Security and then tap Turn On Two-Factor Authentication. On a Mac, you can enable it by going to System Preferences > iCloud > Account Details > Security and clicking Turn On Two-Factor Authentication. For more, see this Apple Support page.

Facebook
Click the triangle button at top right, go to Settings > Security and then click Edit to the right of Login Approvals. Next, click Enable next to where it says that Two-Factor Authentication is currently disabled. For more, see this Facebook help page.

Google & Gmail

Head to Google's 2-Step Verification page, https://www.google.com/landing/2step/, click the blue Get Started button and sign into your account. You can choose to receive codes via text or a voice call. You can also set up and print backup codes, add a backup phone number and set up Google's Authenticator app. You can also sign up to use Google prompt, which sends a notification to your phone that you can simply tap instead of having to enter a code.



LinkedIn

Go to LinkedIn's Security Settings page and click Add a phone number if you haven't already done so for your account. With your phone number added, click Turn on next to where it says Two-step verification is turned off, enter your account password and then enter the verification code that LinkedIn sent to your phone.

Microsoft

Go to the Security settings page, sign in with your Microsoft account and click Set up two-step verification. You can choose to receive codes via email, text or via the Microsoft Authenticator app. You'll also need to create an app password to continue to use Microsoft devices and services that don't support 2FA such as the Xbox 360 and Outlook.com email on an iPhone or Android phone.

PayPal

Log in to your account and click the gear icon in the top right to enter Settings. Click the Security tab and then Update next to Security Key. Enter your mobile phone number and then enter the verification code that PayPal sends you.

Twitter

From the Twitter app, tap your profile icon and then tap the gear icon and tap Settings. Go to Account > Security and toggle on Login verification. You'll get codes via SMS. You can then request a backup code, which you can screenshot to keep handy. For more, see this Twitter support page.

Worksheet #4 - Have you been pwned?

Have you ever looked at whether your data is already available for the taking? And no, I'm not talking about visiting the dark web. This worksheet is somewhat of a continuation from the previous one in the sense that a data breach usually means your name, personal information, username, and/or password are released for all to see. Breaches are one of the main reasons why you should use a different password for every single website with zero exceptions.

Keep in mind that breaches vary in severity. Some can leave nearly every shred of your personal data and deepest secrets out in the open for all to see. Others may *only* reveal your username/email and password. Although breaches with passwords receive the most notoriety, they can still be an issue even if your password isn't revealed. For example, have you ever wondered how you end up with so many spam emails? It's highly likely some bad guy just downloaded a user database from a past data breach because they know it contains "good" email addresses. Other breaches, such as the Facebook security incident in late 2019, exposed your name, phone number, and other minor details. Maybe they are partially to blame for some of those car extended warranty calls?!?!

The website, Have I Been Pwned, has been around for quite a while and it is well-trusted by numerous people including law enforcement around the world. It is a fantastic, free resource. The way it works is the website author/owner receives breach data from different sources, he verifies whether the data is legit, and he then uploads it in a way that you can check whether you are in the breach all from a simple form on the website. No sign-ups necessary! He also has ways for different products such as password managers to programmatically check whether your password was in a breach without actually sending your password... How cool is that? The next question that always comes up is "What about their security?" Well, it's very good, but in the off-chance they were breached, what's there to lose? Keep in mind that ALL of the data is readily available elsewhere.

https://haveibeenpwned.com/

The website is simple to operate. Just type in your email or phone number and it quickly reveals whether you have been a part of a breach as shown in image 1. And yes, if you have multiple email addresses, you can and should check all of them. Perhaps you've had the same email address for well over 10 years? There's a near certainty you are going to be a part of multiple breaches. As mentioned, breaches vary in their severity and the website even shows what data was revealed in each respective breach. Look through the results and REALLY think about what you are looking at. For example, if you see you were part of the LinkedIn breach from 2016 as highlighted in image 2 below, have you changed your password since then? Do you use that

same password for other websites? If so, then this new knowledge should prompt you to change that password on all of the sites you use it on. Maybe a good password manager can help you with all of those new, complex passwords you need to remember? <See #3 above>

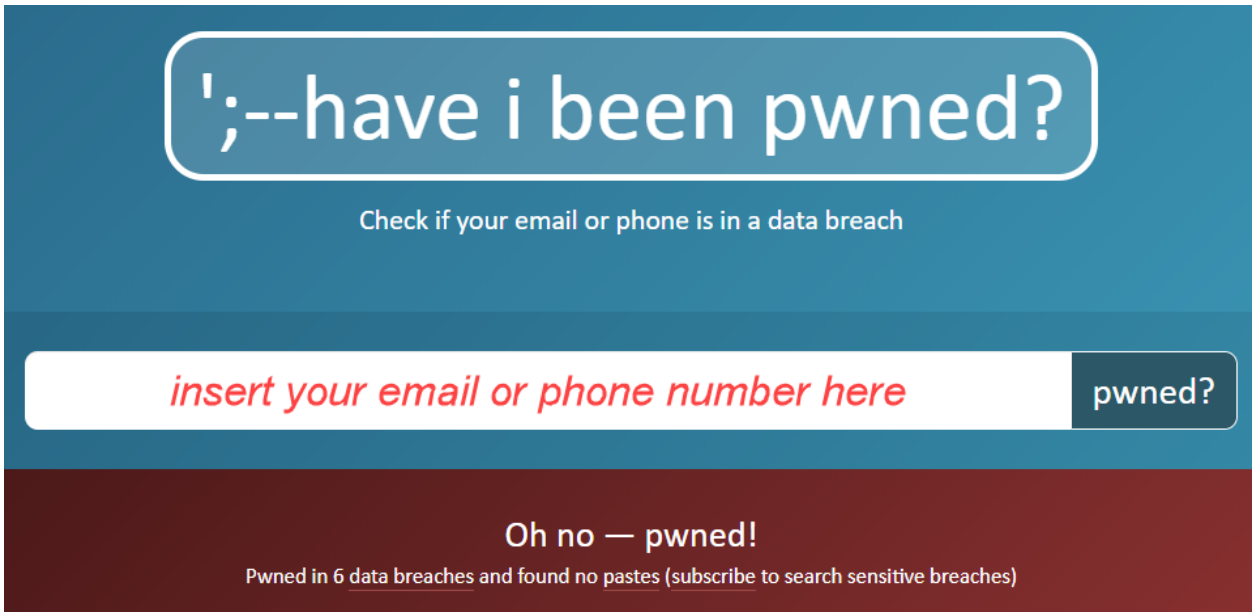


Image 1 - Easy to operate. Just type your info in and hit enter!

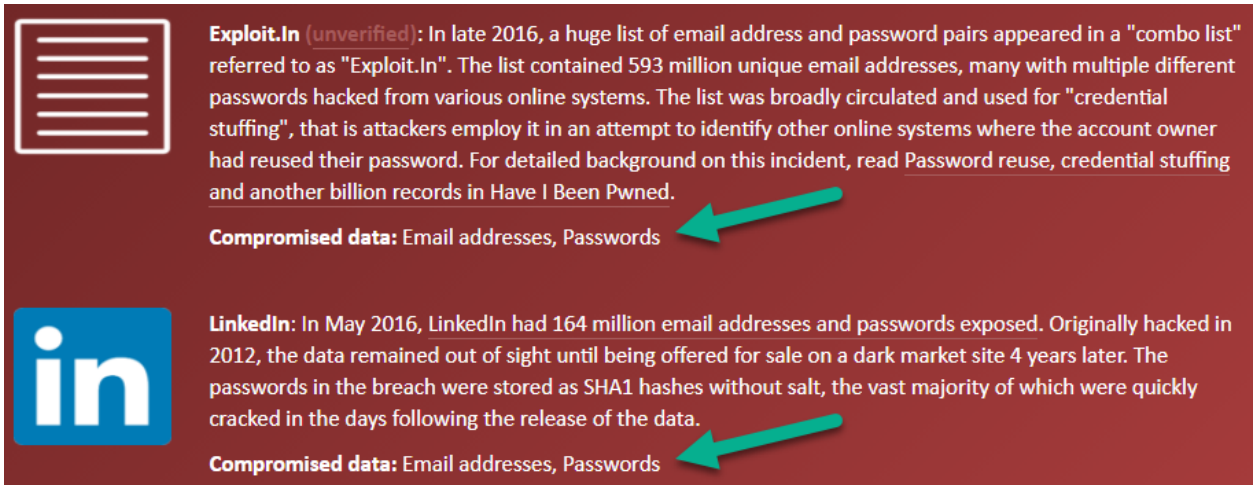


Image 2 - Pay attention to what data was stolen in the breach

Worksheet #5 - Sharing is caring

Well, you've made it to worksheet #5. Yay! There's a good chance some of the prior worksheets took a fair amount of time to complete. The good news is that I'm going to let you off the hook on this one. It's a little easier than others, but it is **oh so important** to the cause.

As we discussed in the presentation, cybersecurity awareness training is a must for everyone. The only issue is that most people never set aside a few hours to learn more about the basics. Take a moment to think about what you learned in this training and these worksheets. What did you learn that you didn't know beforehand even though you've used the internet and/or email for the past 5, 10, or even 20 years? Did you learn how to better spot phishing emails? Maybe you finally took the step toward implementing a password manager or 2-factor authentication?

Where exactly am I going with this? Your mission is to share this training.

First, share it with at least 2 people who are retired. Are older folks the only ones getting targeted? Of course not, but I can tell you that an overwhelming number of the people who came into our office to tell us how they were scammed were *not* using computers or the internet their entire life. And it's absolutely heart-breaking to hear one story after the next wishing they would have taken an hour to go through the training and become more cyberaware.

If you work at a company, then talk to your HR, manager, or owner about adding security awareness training to your company policies as a requirement. No business is too small! It's not uncommon for cybersecurity awareness training such as this one to become a part of the new employee onboarding process or even yearly employee training. Cybersecurity awareness must become a part of your culture and it must be everyone's job.

Last but not least, remember that you should test your newfound knowledge. We have free quizzes on our TreeTop Security website. If you are a business and you want to go a little further, you should also consider periodic phishing assessments. A phishing assessment is where you test your employees before the bad guys do. We perform phishing assessments for businesses that take part in our Peak cybersecurity platform, but keep in mind that there are a lot of options in the marketplace. Find someone you trust and go for it... It will be money well-spent!