Good Evening
Welcome to Tech Tip Tuesday (T^3) for 5/7/19 T^3
Last week at the individual faculty meets many of you shared stories of loved ones being scammed. Since last Wednesday many of you have continued to share stories of scams.

So, todays Tech Tip Tuesday is dedicated to taking to our parents about safety

Below ae tips taken from the SecureMac website.   Link to the SecureMAc Posting and a link to a podcast on talking to our parents on Computer Security
There is a lot here, but well worth the read and conversation with a loved one.

Checklist 62: Talking to Your Parents About Computer Security

Posted on November 9, 2017

Remember back when you were a kid, and someone sat you down to have “The Talk”? It might have been your parents, or it could have been a teacher, but we’ve all been through the experience of learning about “the birds and the bees.” It’s a pivotal moment, and learning about the facts of life can be, well, life-changing. It’s also essential for keeping you safe as you continue to grow up. Well, now you’re grown — you’re older and definitely a little wiser. It might be time to sit down with your parents and have your own version of The Talk with them — the one about the phishers and the hackers. In other words, you should speak to them about how to stay safe with technology

It was all much easier when we were younger. Our parents knew that they didn’t know much about computers, and it was easy to continue in life without them, so they ignored them. Over the past couple decades, computers have grown easier to use, smartphones have slid into our pockets, and tablets have ended up in our hands. On a general level, these things might be safe — but it’s how your parents use them that can get them into trouble.

That’s our subject for this episode of The Checklist: educating your parents on how to avoid security problems through “The Talk 2.0.” Today we’ll cover:

1. 1. Password safety
2. 2. Avoiding phishers
3. 3. Steering clear of harmful downloads
4. 4. The importance of security software
5. 5. How to avoid online scams and disinformation

1. Password safety for your parents

Here’s a good place to start — passwords. If your parents use tablets or smartphones, hopefully they’re already familiar with using passwords in the first place. It’s up to you to make sure that they also become familiar with why good password security is so important. This topic is so fundamental that we chose to cover it right away, not long after we started The Checklist. If you want a refresher on anything we discuss in this section, or just to go into more depth about password security, hit the archives and check out the show notes for Episode 8.

The first thing you should begin with: the importance of having strong passwords to any online accounts. It’s helpful to use analogies to keys and locks here since that’s precisely what passwords are. If your parents use a password that is complex, it makes it that much harder for someone to guess the right words to enter their account. Compare it to a lock that a burglar can pick with ease. You wouldn’t want to use a lock on your front door that anyone could break into with only a little bit of effort. Instead, you want to choose something that will keep the bad guys out. That’s why it’s so important they take the time to make good passwords.

While on that topic, it’s also an excellent time to discuss the importance of avoiding password reuse. We know it’s not easy — remembering all those passwords can be a pain, and we’re also fond of saying “don’t write your passwords down.” But unique passwords are a necessity today. Ask your parents to imagine what it would be like if they had a shed and a storage unit in addition to their home.

What if a burglar stole a key to their front door? That they can access their home is bad enough — but they could also take that key and break into many other places, too. That’s the risk when you reuse passwords. If one site gets hacked, but your parents use different passwords everywhere, the bad guys won’t be able to get very far.

So, you want them to know they need to make strong passwords, and they need to make a lot of them — but they also need to keep them safe after the fact. Bring up the fact that it’s important to never share passwords with other people for any reason. When you do, you risk allowing a stranger or even the bad guys to get into your accounts. There’s never a reason for any business to ask for your password during technical support, either.

Let your parents know that when they deal with a legitimate support line for a company, the technician on the phone doesn’t need your password to access your account. They can do that already on the back end. In place of a password, some companies will provide a security number like a PIN for identification instead. This number is okay to share. Otherwise, they should keep those passwords safe and secret!

At this point, your folks might be starting to worry that they’ll never be able to keep track of all this — why should getting into your accounts be so complicated? Luckily, it doesn’t have to be; now’s the right time to bring up a password management app. With this software, they can do everything they need. They can do all the stuff you just explained within the app: they help you to create robust passwords, and they make sure you don’t have to try to remember those long garbled string of letters and numbers.

With an app they can track all their passwords across all the many sites they use. It’s a “set it and forget it” style of software, too. Once it’s set up, it keeps on working, and many provide anti-phishing protections to alert users when a website isn’t hosting a legitimate form. For those of you whose parents are Apple users, we suggest that they use the 1Password app, or barring that, choosing to use Apple’s built-in iCloud Keychain. Both solutions will help keep your parents safe.

2. Staying safe in an online ocean full of phishers

Phishing is the topic you should look to hit next. To stick with the key analogy, you can install very strong locks, but the bad guys would love a chance to steal your keys. If they could trick you into handing them over, that would be even better. That’s what phishing is all about — and once you explain that it’s spelled with a “ph” and has nothing to do with angling for a bigmouth bass, you can start breaking down what it is and how they can stay safe. Like password safety, we’ve covered this topic in a previous episode. Revisit it, or check it out for the first time, by listening to Episode 37 in the Checklist archives.

Phishing is the domain of online con artists, plain and simple. These bad guys want to trick us into giving up their personal information so someone else can get into their account. In many cases, it might be something as simple as trying to trick you into giving up the login information for your online bank. It’s the easiest way for someone to steal your funds online, after all. While spotting that kind of trick might seem simple, it’s not always so easy for everyone else. Other phishers might try to coax out information such as your routing and account numbers, and they use some pretty sophisticated fake sites to make their attempts. While being careful with this info is easy to explain, you need to go deeper — phishers can be very crafty.

Explain that a phisher might try to receive information that, at first glance, doesn’t seem very important at all. This data could include their date of birth, a mother’s maiden name, their hometown, and all kinds of other, similar information. Point out that with this info, the phishers can easily start opening new accounts in their name. It’s a one-way ticket to identity theft — something your parents may be familiar with already.

So where should they put up the most defenses? Where should they try to expect these attacks to originate? Phishing today comes in many different disguises, but by far the most commonly used one is still our good old friend: email. It’s not always easy to spot phishing emails, but you can give your parents some essential pointers to make it easier.

In most cases, it’s best not to trust emails that purport to come from your bank or online financial account. Unless you’re expecting these emails — such as a confirmation that arrives immediately after making an online credit card payment — it’s safer to assume they might not be legitimate. Don’t click on the links found in these emails; they could lead to a fake website that tries to phish your information. Instead, tell your parents to check out the bank’s website directly to verify that the email is legitimate. Today, many banks have begun to include security verification in their emails, directing users to manually visit a web address to check the email’s authenticity.

Another key indicator of a phishing email are spelling mistakes and bad grammar. Many phishers originate in countries where English is not a native language. The use of broken English in an otherwise official looking email is a key indicator that something may be fishy!

In other cases, your parents might see a pop-up ad, or run into a website that demands they call a phone number or install a piece of software for help. Often, these pages and ads come with terrifying and dire warnings that are meant to make you think you have no choice but to act quickly. The ad might say that dozens of viruses infect the machine, and only by downloading special software right then can their data be rescued. Naturally, these are all fake. You should stress that such random warnings are never legitimate.

Finally, it’s important to warn your parents that phishing sometimes happens away from the computer, too. The bad guys could call up their phones — yes, even a cell number — to try and trick them into forking over personally identifiable info. That could be account numbers or even their Social Security number. Callers who claim that you have won a cruise and they just need to verify some information are a common scam. Consider rounding up info on other common phone phishing scams to share as examples.

3. Steering your parents away from harmful downloads

Now that you've covered the basics of being smart with passwords and understanding how to spot phishers let's pull back to the bigger picture of the Internet in general. With smartphones everywhere and sites such as Facebook acting more and more like a portal to the rest of the Internet for some users, it's critical for your parents to understand some basic facts about the Web at large. Covering these important pointers can not only keep them safe, but it can also prevent all kinds of tech support problems later down the road. Those are frustrating for everyone involved, so why not avoid the issue altogether?

Downloading something you shouldn't is the most common way computer users end up with problems on their machines. It doesn't help that there's no end to the number of places that offer up things to download these days. It's not like in the old days of dial-up Internet when downloading a one-megabyte file meant a serious time commitment. Instead, files finish in a flash, and it only takes one click to install something that wreaks havoc on your parents' system.

So important fact #1 about safe web browsing: anyone can participate. That means anyone can make an app, and anyone can make a website, and anyone can put what they want up for download. Explain that just because something shows up in the results on Google doesn't automatically make it safe. Downloading and installing all kinds of random software based on Google searches is a fast way to end up with a virus or some other form of malware. Let them know they need to exercise a healthy skepticism to stay safe on the web. Just like you can't trust everything you read, you can't trust everything on the Internet.

Now is a good time to warn them about websites that try to force users to install software to access the site. We see this a lot with fake "streaming" sites that encourage users to install a "video player" to watch the latest blockbusters right in their browser. These messages are always a direct link to malware — you're not going actually to find those movies on the other site. Likewise, browser toolbars are unnecessary and extraneous; they don't need to download and install any of them to get the functionality they need. Find out if they have any questions about their web browser that you can clarify.

It's good to let them know how to avoid these problems — but what happens if they make a mistake? We all trip up from time to time. Explore with them what steps to take if they've accidentally downloaded something that now seems dangerous or otherwise unsafe. It might happen on purpose, or it could be a "drive-by" download, where a website automatically forces the browser to start downloading.

Tell them not to run anything they download this way. Don't click on it or open it; instead, delete it from the machine altogether and don't go back to the website from which it came. If they avoid letting the software run, they won't have to worry about a malware infection. If they did run the software, though, and installed some mystery software, it's time for a thorough system scan with their security software. This scan can help to root out any malware that arrived via the download.

Now is an ideal moment to touch upon the fact that the phrase "there's no such thing as a free lunch" applies to the Internet, too. No matter how much we might want to find "free" copies of expensive software, it's a risk that's not worth taking. Not only is downloading copies of commercial software or copyrighted material deemed piracy, but it's also a great way to infect yourself with malware. The Internet police won't come banging on the door for pirating software, but that doesn't mean there aren’t consequences. Rather than deal with the trouble, it’s best that they just stick to all the legitimate avenues for purchasing software or consuming digital media.

4. The importance of setting up security software

Since we mentioned running security software in response to a shady download, we’ll turn to that topic next. At this stage, it’s smart to start steering the conversation towards security programs and why they need to have this software installed on their computer at home. Expect to hear some complaints — we’ve all had bad experiences with antivirus software at one point or another. From slowing our computers way down to causing serious system problems, there have been products in the past that didn’t work as well as intended. Today, things are very different. Before you dig into that subject, though, go over why they should install security software in the first place.

Malware isn’t a problem for just one platform — there’s bad stuff out there that can affect you whether you’re a user on Mac or a PC. The threats are real, too; you only need to point at ransomware outbreaks or high-profile malware events that crop up in the news to show your parents that. After showing some examples of the potential damage, touch upon the ways security programs help. Point out they offer an extra layer of protection beyond what their computer provides on a fundamental level. If your house has its doors, windows, and locks to keep out the bad guys, it can also have a security system. The concept is the same.

That said, not all security software packages are equal. Some programs out there are barely a few steps above useless — others have so much bloat and unwanted add-ons that they’re almost like malware in their own right. Like everything else on the web, it will require your parents to put in some effort at sleuthing out the best solution. You may even have your own experience that allows you to make a recommendation to them. Installing security software created by professional, reputable vendors is the best way to go. Searching for “antivirus app” and downloading the top result on Google or the App Store is not. When you do your homework, it’s much easier to find the software that works for your needs.

When your parents search for security software, they must be very wary of any solution that only offers a free product. If that software doesn’t receive regular updates, it’s not going to keep them safe from the latest threats. While many of the major providers, especially for Windows machines, do provide free versions for home use, many more require a monthly or yearly fee for service. Again, look towards products from professional, reputable vendors.

Finally, be sure to remind your parents that they need to actually run the software once they install it! Just having it lurking on the hard drive isn’t enough to provide magical protection. Disabling it is no good either. Like we mentioned: expect some complaints during the initial learning stages. Some users turn off their security suite because they think it slows down the machine, while others never configure software in the first place. That can lead people to believe the software doesn’t work at all.

Offer to help your parents configure the software so it provides the appropriate level of protection. They can even choose to set up regular scans for maximum protection. To avoid interfering with daily activities, just schedule to run at night — they’ll stay safe and protected that way.

5. Avoiding scams on the Internet

With a good security solution in place and a foundation of other knowledge coming together, it's worth spending some more time discussing the potential scams and threats your parents might encounter when they browse the web. As older computer users, they're especially at risk as many scammers target individuals like them based on their less-developed computer skills. The only way to fight back against that is through education and information.

There are all kinds of pitfalls out there on the web, and it can help to go over what your parents should avoid. You may know that these things are all fake, but you also have years of Internet experience — and maybe some mistakes of your own that taught you lessons. So, what are the scams they should know to avoid?

The pop-ups and ads that claim your machine has active malware infections, as we mentioned, are always fake. Likewise, websites and Facebook ads that claim you can receive a free iPad or other high-value item for completing surveys aren't real. In fact, these are often phishing endeavors that collect all types of information about the users. At the very least, you might be handing your email straight over to a spammer.

The scams can come into your parents' email inbox, too. No matter how many years go by, there's still a Nigerian prince out there who just needs some of your time and money to access a huge amount of money to share with you. Ignore these bogus emails — use the old axiom "if it's too good to be true, it probably is."

Away from the computer, it's important for your parents to beware unknown callers on the phone, too. It's unfortunately easy to find someone's phone number online these days, even cell numbers, especially if you aren't strict about your social media privacy settings. Scammers know this, and they're looking to use this to their advantage at all times. Some scammers just use robo-calling systems, which call every number sequentially looking for valid phone numbers. Here's one scam that everyone should know to avoid.

This is the scenario: one of your parents receives a phone call from an individual who claims to represent the IRS. They state that an audit of their records shows that your parent owes thousands of dollars in back taxes that are now due immediately. If they don't settle up for a fraction of the total amount immediately, they'll be liable for more huge fines or even jail time. Sometimes, the scammer will threaten an arrest right away — they might even say the police are ready with a warrant.

Hang up the phone! The IRS would never contact an individual taxpayer this way, nor would they demand money in such a shakedown. Scammers also use this method via email and even by regular mail. As always, when in doubt, tell your parents to try to verify the information with the business or agency in question.

Who you dial is just as important when it comes to safety and avoiding scams. Many of the bad guys have taken to trying to set up fake technical support lines for major companies or popular products and brands. When you call in, you might get some vague help, but it's all a disguise for stealing your info. If your parents need to get a hold of a company, tell them to avoid blindly trusting the first phone numbers that Google suggests.

Instead, they can just head directly to the company website and find their contact page. That way, it's easy to know you're always calling the right number. With so many scams out there, it's tough to guard against them all, but a skeptical mind and a careful approach can make things much safer.

Once you're finished having these discussions with your parents, be sure to ask if them if they have any questions about what you've covered. Be patient and take the time to explain your answers clearly and concisely; remember, no one starts out knowing everything there is to know about computers and digital security.

Once your discussion wraps up, it can be helpful to leave behind a hard copy with the important information so your parents can review it as necessary. Write down some of the tips and tricks we discussed in today's episode, or print out a copy of these show notes. Whatever you do, remember to make yourself available for questions and concerns. It always helps to know you have someone to turn to with computer questions.

That covers everything we have for you this week! Did today's discussion bring some questions or curiosities to mind for you? Is there another subject that you think we should hit on the show? We'd love to hear all about it directly from you — so just send us an email to Checklist@Securemac.com to share your thoughts.