USING PUBLIC WI-FI

When it comes to using public Wi-Fi, there's one main rule: don't do it. Public Wi-Fi is a very convenient amenity at your local Starbucks or at the hotel where you're staying, but there are too many ways that the bad guys can get between you and the network and gain access to your personal information when you use public Wi-Fi. Even if there is a password to the network, it's not safe. Use cellular data or a virtual private network if available, but never trust public Wi-Fi.

INTERNET OF THINGS DEVICES

We all seem to use them. Whether it's security cameras, doorbells, thermostats, or baby monitors, our lives are becoming more dependent on internet connected devices. The convenience is wonderful, but the security issues of using these devices are significant because they're a gateway into the network. The safest solution is to not use these devices - but if you do, make sure to understand the security risks and perform the necessary steps for security measures such as immediately updating patches. Remember: the security of IoT devices is as important as their function.

WHAT IS THE "DARK WEB"?

There are three parts to the world wide web: the surface web, the deep web, and the dark web. The surface web is everything that's publicly available and accessible through a normal search or by typing a URL into a browser. The deep web is all the content on the internet that is not indexed by standard search engines, such as online banking sites or web mail. Then we have the dark web, or dark net. The dark web is a totally different animal in that it's only a tiny fraction of the overall web and is only accessible through specialized software such as the Tor browser. People can remain anonymous on the dark web, which makes it appealing to a number of characters. The dark web is used to conduct questionable and even illegal activities such as child pornography, illicit drugs, firearm sales, and many others. If someone's a bad guy, the dark web will be where they do their online bidding.

THE SECURITY PERILS OF SOCIAL MEDIA

Obviously social media is a huge part of everyday life, and that's not going to change anytime soon. The bad guys know this and have figured out some clever ways to take advantage of it. Someone can assume the identity of a corporate customer or an executive and manipulate corporate social media platforms, or even plant malicious links at popular places to visit on social media. Many times, scams centered around surveys or winning prizes are used, and when you see a story that Brad Pitt has been killed in a terrible helicopter accident, think before clicking on the link. The moral of the story is… be ever cautious when using social media platforms, because things are not always what they seem.

THE NEED FOR CYBER INSURANCE

If you have a network with sensitive information on it, then you need to have cyber insurance. The costs of a breach are at best significant and at worst devastating, and insurance to help your business recover is an absolute must. There are many nuances to cyber insurance, so make sure to engage an insurance professional who's well-versed in this evolving insurance line. But know this: if your enterprise does get breached, and you don't have robust cyber insurance, survival will be a challenge.

MOBILE DEVICE SECURITY

Most people don't realize that their phones, tablets, and other mobile devices are a huge target for hackers. Instinctively we think our mobile devices don't have the same security concerns as our desktop work computers, but that's far from the truth. Hackers love to target these devices, and, as users, we must employ the same security practices, such as data encryption, strong passwords, updating all security patches, and dual authentication. Treat your mobile devices like super computers - because that's basically what they are.

THIRD PARTY VENDORS

If your business has third-party vendors with access to your network, you have an entirely new set of security issues to contend with. The infamous Target retail hack occurred through their air conditioning vendor. Because they didn't pay enough attention to the vendor's security measures, Target's running cost is over 500 million dollars. Cyber criminals always find the easiest network access point, and many times this is through a software vendor or other type of vendor. It's critical for every enterprise to do everything possible to get a handle on the security posture and protocols of all third parties you deal with. No exceptions.

HOW TO RECOGNIZE A PHISHING EMAIL

There's no question that phishing emails have become more and more sophisticated and harder to detect over the last few years, but there are certain things you need to watch out for to determine if an email is actually a phish. First, check the actual email address of the sender to make sure it's from the source that the email sender says it's from. Also, hover your mouse over any links in the body of the email to see what the true source of the link or attachment is. Be wary of any email that uses generic greetings, demands immediate action, or has misspelled words. Finally, if you have any doubt, call the sender to verify its legitimacy. Remember: you can never be too careful with electronic communication today.

HOW TO RESPOND TO RANSOMWARE

If you're hit with ransomware, you must act quickly to contain the problem. The first course of action is to disconnect any infected machines and disable any shared networks. You can Google the information on the ransomware screen to determine what type of ransomware it is and the specific appropriate actions related to that strain. Make sure the ransomware is removed from all machines by wiping their hard drives, restoring factory settings, and using back up files to restore the data. And if at all possible, never pay the ransom, since that just makes you a more likely target for future attacks.

CRYPTO-JACKING

For crypto-currency transactions to take place, miners have to validate the transactions. The mining process takes huge amounts of computer processing resources, and many of these miners have decided that they would rather hijack other people's networks than use their own. When that happens, it's called crypto-jacking, and it's a rampant problem today. If devices on your network are acting funny or running very slow, you just may unknowingly have a crypto-jacker on board and need to get him out of your network.

SMISHING

As we've become more aware of phishing schemes on our personal computers, the bad guys have moved towards executing their schemes on our mobile devices. For some reason we tend to think of our phones or tablets as safer than our desktops, but that's far from the case. Using mobile devices for phishing schemes is called "smishing" and is a widely used variation of traditional phishing. Be careful if you receive links or attachments via text, or if you receive texts from unknown sources. As always, think before you click.

INTERNET SECURITY WHILE TRAVELING

Internet security issues abound for travelers, and it's important to understand and mitigate the risks. Make sure to back up all data before departure, and change passwords both before and after your trip. Disable any auto-connect settings, and don't use public Wi-Fi. Use a virtual private network if possible, and have strong passwords and encryption on all your mobile devices. Don't use public charging stations, minimize location sharing, and use privacy screens. Finally, secure all devices at all times. Remember: you don't want your trip to turn into an online nightmare.

VISHING

Vishing, or voice phishing, is a form of criminal phone fraud that uses social engineering over the phone to gain access to private personal and financial information. Vishing frequently involves a criminal pretending, over the phone, to represent a trusted institution, company, or government agency. You may be asked to buy an extended warranty, offered a vacation, told your computer is infected and you need anti-virus software, or asked to donate to charity. Basically, vishing is a new name for the age-old telephone scam. To conduct these scams, vishers often use modern voice over IP features such as caller id spoofing and automated systems that make it difficult for authorities to monitor, trace or block their activities. They'll stop at nothing to achieve their goals - and use of the good old-fashioned phone is still in vogue. With phones more than ever being a constant part of our lives, it's very important to be skeptical and diligent at all times.

STRONG PASSWORDS

We're required to generate passwords for different applications constantly, and it's important to remember a few basic rules when doing so. One good rule is: "a long password is a strong password." A 12 character minimum is a good rule of thumb. Also, use a mixture of numbers, letters (both upper and lower case), and symbols. Don't share your passwords with anyone, and don't write them down in plain sight. Don't use easy to recognize themes such as your last name or birthday, and use different passwords for every application. Change your passwords often, and use a good password manager to store them. Remember: your passwords are the gateway into many important parts of your life, and you must use good password hygiene consistently.