k_Street Consulting

WHITE PAPER

Best Practices for Security Awareness

k_Street

Security awareness training is like the pre-flight safety speech. You need to know what to look out for and what to do before the emergency happens.

Employees should undergo regular reoccurring security awareness training to educate or refresh their knowledge of various dangers such as using public Wi-Fi, how to spot suspicious emails (phishing), awareness of current scams used to gain information, password techniques, handling of data and media, etc. Some industries such as financial require this training but it is a good practice for all companies. Remember, the end users' vigilance is the first and best line of defense in preventing a breach or loss of data.

The following is a security awareness training discussion on the use and handling of data, maintain privacy and situational awareness for both personal and business environments.

Please note these recommendations apply only to general corporate data access and resources. Governmental or classified data, as well as employee or customer financial data, personable identifiable information, private health information and information related to citizens of the European Union may require greater security measures than discussed here.

Here is a scenario. You are a CFO of a small firm. You come in one morning and waiting in your inbox are 5 emails. One is from your significant other with a subject line saying “check this out” and a link to YouTube. Next, an Amazon order with an invoice attached; another from the IRS requesting W2s; one from your boss saying he needs wiring info, and lastly a Nigerian prince who was “good fortune with you connecting to benefiting financial”. Which is the phishing email?

If you said the Nigerian Prince you are correct, as long as you said all of the others as well. Each one of these is a common threat vector today. Gone are the days of the broken English Nigerian prince shot gun blasting the Internet with his emails asking for your help extricating millions. These days, attacks are very pointed, directed, researched and incredibly difficult to detect.

This paper is on cyber security awareness from both a personal and business aspect and we are going to run through a prescription of recommended best practices along with examples of current threats.

It should be noted that you will never be 100% secure assuming you maintain some semblance of connectivity and identity. While the comments here are meant to help you improve your security posture, they are by no means full proof and everyone’s situation is different. You should seek the council of an experienced IT professional who is familiar with your specific environment and needs.

S.A.V.E

When it comes to protecting yourself from cyber threats, you are the first and most advance line of defense you have. Let’s walk through how you can protect yourself with this acronym:

S. A. V. E

Segment

Authenticate

Vigilance

Everything is a potential threat

Segment

Segmentation is dividing your digital life up. An expectation of threat actors is, “if I can find a crack in the wall then the castle is mine”. There is a good chance you most likely use the same logins, the same passwords, store your data in the same location, and typically use one device for both personal and work. Therefore, if they successfully break into one thing, they will most likely be able to break into others.

At a minimum, you should have a unique password for every login and you need to change it at best 4 times a year, at least twice a year, but no less than once a year. The primary reason for this is, over time, your password will be leaked through various means out of your control. The longer you keep the same password for any resource, the more likely it will end up on the “dark web” associated with your email address then potentially used in a breach. This is exacerbated by the unfortunate practice of

using the same password for multiple resources. A common technique is for bad actors to gain a user name such as an email address and an associated password from a resource with expected weaker security and then attempt to use those credentials on a more secure login of a different resource. An example being criminals capturing your LinkedIn login information from breaching that site, then using the information to gain access to your email, then using the access to your email to reset your password to your bank account.

Your probable response to this is one of the more common complaints- "I have too many passwords to remember". So let's take this moment to discuss passwords. You may have heard in the news about how long passwords and changing passwords is now considered bad form and the original designer of these standards is now speaking out against them. From a professional aspect, this is a disheartening concept because the reasoning behind long and complex passwords being weaker is not some inherent flaw in the passwords, it's the flaws in humans. That humans won't remember their passwords so they write them down or that when they change them, it moves from SportsTeam1 to SportsTeam2. The fact of the matter is, from a technology standpoint with the automated methods used to break in, complex pass phrases are critical. Note that we said pass phrase that time and let's talk about how to create a complex one that's easy to remember and unique to all websites.

The Password Algorithm

First, use a phrase rather than a word. A technique to breaking a password is to use a dictionary of common words. Generate a phrase that you will remember. For our example, let's use "It was the best of times, it was the worst of times". Now, an easy to remember sentence, but we don't want to have to type in that whole phrase. What if we took the first letter of each word?

"It was the best of times, it was the worst of times" gives us "iwtbotiwtwot". It looks complex but each morning all you are typing in are the letters and you say to yourself the easy to remember, "It was the best of times, it was the worst of times". Keep in mind, this is just an example, you can use a much shorter phrase, but note by the end of this process, it is best to have a password around 10 characters. Now, while "iwtbotiwtwot" looks complex to us, by computer standards it is not and it's computers that are the ones doing the actual act of cracking your password, not a human.

To increase the complexity, you'll want a number and a symbol in there. Let's say 01 because that phrase was on the first page of the book "Tale of Two Cities". There's a period at the end of that sentences so let's use a period as special character. We recommend putting the symbol at the end of the entire passphrase as some websites do not permit special characters so it's easy to drop off if that's the case. Now we have "iwtbotiwtwot01."

You now have an easy to remember 15 character, strong complex password.

But we still don't want to use that same password on every site. So, what's unique to each site? The website address. We don't want to have to type the whole name, so let's just take two letters from that domain name. And to keep from being totally obvious, let's use the last two of the primary domain name and we'll capitalize them to get our 4th category of complexity. You'll need two letters else you'll see a surprising number of repeats. For your network password, you can use letters from the company name. For example with the site www.outlook.com our passphrase is now "iwtbotiwtwot01OK." Again, keeping the special character at the end.

And voilà. We now have a long, complex password that's in fact easy to remember, and while it will be unique to every site you log into, it's still for all intents and purpose, only one password. In short, it's just a base passphrase and two letters from the resource you are accessing. When it comes time to regularly change your password, you can rotate any of the 32 symbols found on a standard US keyboard.

Your business should have a password policy that enforces the use, length, and changing of passwords. For more developed networks, you should set an age and history of passwords as well so users are not able to quickly cycle through just to keep from changing passwords. Passwords should be used not only on computers, but phones and tablets as well. Considering your email and contact list on those devices are just a valuable as on your computer.

Another measure that should be taken based on the "Segment" concept is to keep work devices and personal devices separate. Work on your work computer, personal on your personal computer. About 70% of breaches our firm has investigated started because of someone doing something non work related on their work system. Personal emails, Watching YouTube, going to Facebook, reading the news, etc.

Your business should also use segmentation as well in relation to job functions and data. Data saved should be segmented on a need to know basis. The staff should only has access to the data they need to have access to. This is not just a classified data issue, but also, if one person was to become infected or compromised, then not all data is compromised.

Same concept goes for job functions. It should require more than one person to be able to access or authorize financial transactions. Besides being a failsafe, this also promotes honestly as fraud would require collusion. This is obviously dependent on available resources.

What is probably going through your head right now is a sense of burden.

Yes.

Security and convenience will always be diametrically opposed. The same is true for privacy. We trade privacy for convenience. You will have to draw the line between what you are willing to expose versus how much effort you put in based on the expense of mechanisms and labor compared to cost of loss in revenue, regulatory fines, and clients.

We had a client, a financial brokerage firm where the president and CEO had a 3 letter password because he was too busy for anything more complex. That is, until we helped him realize that the 10 seconds he saved could cost him hundreds of millions of dollars should his account be breached.

Authenticate

In cyber security, authenticate usually means logins verifying that a person is who they say they are, but in this case we mean YOU need to do the authentication. You need to make sure data, email, even thumb drives, came from the source you think it did. If you find a thumb drive placed on your desk, ask around who put it there before looking at what's on it.

If you get an email from someone you know but with a link or attachment and no message, it's ok to send them an email asking if they really meant to send it. When in doubt, delete. If a person sent you a legitimate email that looks suspicious and you don't respond, they will follow back up with you. One note here, whenever you are suspicious of any email, obviously don't open it, but if you do, don't use the reply button. Create a new email and manually type in the address. Reply addresses can be spoofed.

Use the concept of the writer's 'voice' when authenticating emails. When communicating with someone you know, or dealing in a familiar circumstance, you know the writing style or 'voice' of that person or that circumstance. Use that as a form of authentication. For example, if a person is normally personal in their email greeting, "Hey Bud" but you receive email from them "Dear Mr. Smith", then the 'voice' is off. That is a flag. We had another personal financial advisor who received an email asking for help transferring money. Just from a comment saying "Kindly reply", our client immediately knew something was not right. It was out of character for this customer to say such a thing. We'll demonstrate a real world example of 'voice' shortly.

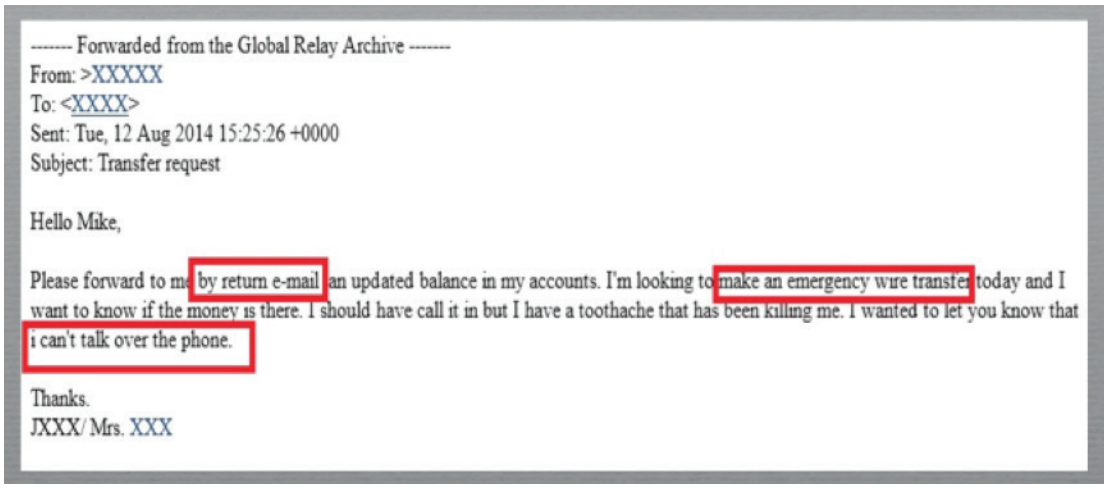
In business, have fail safes in place using authentication for various tasks such as establish a policy that says any financial transaction over X dollar amount requires a verbal confirmation as a second factor of authentication.

A very common technique used these days is for a threat actor to do some incredibly diligent research on your firm and then, using spoofing techniques, forge an email from the right person, sent to the right person, using just the right phrasing to request the right information to wire money or click on a link for an attachment. We had one client, a not for profit, that lost their entire years funding in such a scam.

Typically these emails will be from quote unquote the CEO or president of a small or medium business, and will be sent to the financial person of that company saying there is some sort of time critical issue or emergency requiring them to wire money and asking for the information.

Last year, over 81 million dollars was stolen from one bank in India using a similar technique. In that situation, the bad actors got into the network first and then just monitored emails for over a year until they were able to piece together the procedures used to for making transfers. With that information they then simply mimicked the process.

Here are some examples of actual emails that a client received that demonstrates both this technique and what we mean by "voice".



------- Forwarded from the Global Relay Archive -------
From: >XXXXX
To: <XXXX>
Sent: Tue, 12 Aug 2014 15:25:26 +0000
Subject: Transfer request

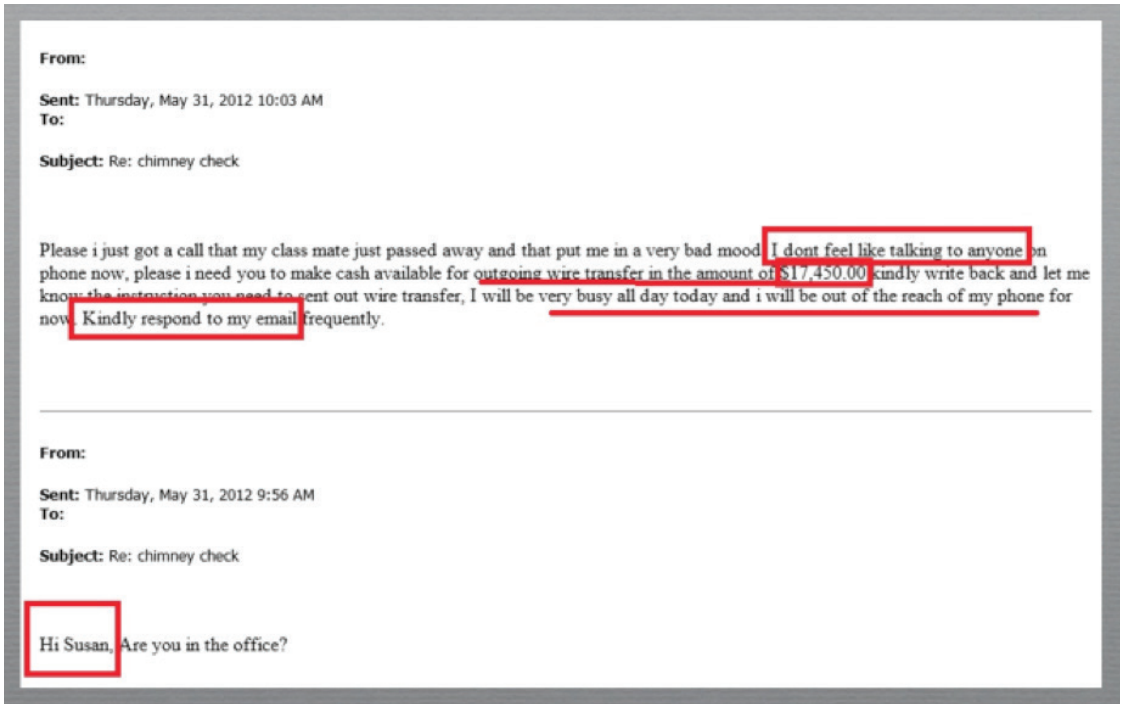
Hello Mike,

Please forward to me by return e-mail an updated balance in my accounts. I'm looking to make an emergency wire transfer today and I want to know if the money is there. I should have call it in but I have a toothache that has been killing me. I wanted to let you know that i can't talk over the phone.

Thanks.
JXXX/ Mrs. XXX

A common technique is to cut off all forms communication other than this email thread. Note the "I can't talk on the phone" Also, note the direction to use the "return email". This goes back to what we were saying about creating new emails so you know where they are going to. Sometimes threat actors will use a display name but different address.

Next, let's look at this thread. First, note the "Hi Susan". This attacker researched who was the right target at the firm for this email. Next we see "the ask". Note the specific amount rather than a round number like 5000 or 10000. Others may get very detailed, down to the cent, with a message saying that it's for a specific need to make it seem more personal. And again, the cutting off of communication.



From:

Sent: Thursday, May 31, 2012 10:03 AM
To:

Subject: Re: chimney check

Please i just got a call that my class mate just passed away and that put me in a very bad mood I dont feel like talking to anyone on phone now, please i need you to make cash available for outgoing wire transfer in the amount of $17,450.00 kindly write back and let me know the instruction you need to sent out wire transfer, I will be very busy all day today and i will be out of the reach of my phone for now. Kindly respond to my email frequently.

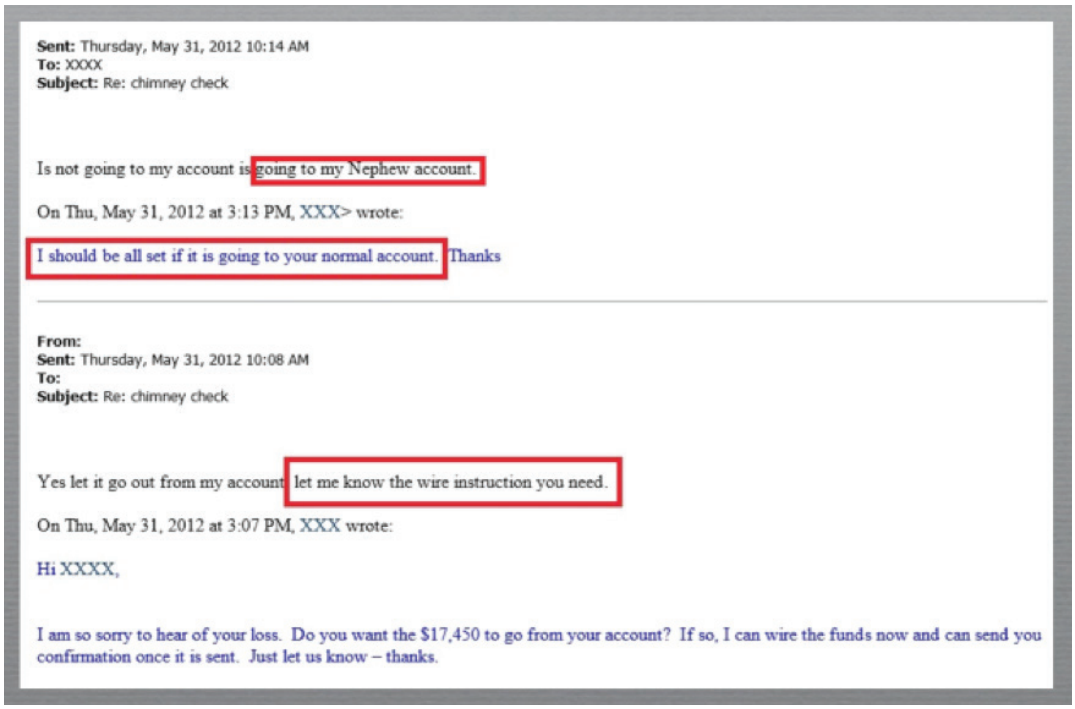
From:

Sent: Thursday, May 31, 2012 9:56 AM
To:

Subject: Re: chimney check

Hi Susan, Are you in the office?

As we follow the thread reading from the bottom up, we see that Susan is following proper procedure. The threat actor offers the wire account to send to and she replied that she will use the information they have on file because Susan knows that's been verified.



Sent: Thursday, May 31, 2012 10:14 AM
To: XXXX
Subject: Re: chimney check

Is not going to my account is going to my Nephew account.

On Thu, May 31, 2012 at 3:13 PM, XXX> wrote:

I should be all set if it is going to your normal account. Thanks

---

From:
Sent: Thursday, May 31, 2012 10:08 AM
To:
Subject: Re: chimney check

Yes let it go out from my account let me know the wire instruction you need.

On Thu, May 31, 2012 at 3:07 PM, XXX wrote:

Hi XXXX,

I am so sorry to hear of your loss. Do you want the $17,450 to go from your account? If so, I can wire the funds now and can send you confirmation once it is sent. Just let us know – thanks.

The threat actor then tries to redirect to a non-verified location, the "nephew's account" which he would provide wire information for. At this request Susan correctly follows procedure and requests verbal confirmation.

From: XXX@gmail.com
Sent: Thursday, May 31, 2012 10:20 AM
To: XXXX
Subject: Re: chimney check

Please try understand me am really in bad mood and i put my phone off for now. go on and send it out i will call you later in the day let me try get there and know what really happen.

On Thu, May 31, 2012 at 3:18 PM, XX> wrote:

I need to talk to you if that is ok. Can you please give me a call? Thanks,

Here the bad actor insists on the cutting off of secondary communication and note the emotional trigger. This is playing on how we function. We all want to please our clients and it's common in American service industry culture that we'll skirt rules and cut corners to make our clients happy. Susan was able to correctly shut this down before a serious breach occurred because she followed the proper procedure of verification and was vigilant.

One thing that Susan also said at the time was that the voice of the client was not right, that the phrase "Kindly reply" was not something she would ever expect this person to say. It just wasn't their style.

Mind you, it comes from knowing their clients on a one to one basis and the relationships they built, but you can see it also in emails where you don't know the person but you do know the circumstance such as where a person is too formal or too informal or too detailed for a particular type of business request.

Be suspicious of any form of communication asking for any information or funding even if it appears to be coming from a trusted source. Today's cyber frauds are incredibly sophisticated.

Vigilance

This previous example feeds into our next leg, Vigilance. It was Susan's vigilance that raised her eyebrow rather than just rubber stamping her job. Vigilance is your primary line of defense. You always have to be on your guard. It's those moments when you are lax- lax on security, lax on your surroundings, or just in a rush- that you will miss tale-tale signs that could have warned you. Anticipate a breach no matter what you are doing.

No one should believe they are too smart to be conned. We are all susceptible. At the height of the Nigerian Prince fad, there was a report of a woman in upper management of an accounting department. She received a "prince" letter and proceeded to embezzle nearly $80,000. Her thought was she would use this money to seed the account she needed to set up for the prince to transfer the money into (that's how the con runs) and when she got her 20% of his millions, she would just put the money back she "borrowed" and no one would be the wiser.

This fell apart NOT because someone detected the embezzlement while it was happening, rather long after the con was completed and the money was stolen from her and she was no longer able to conceal the missing funds. That means she did a good job at the embezzlement part. She was smart enough for that, and yet, still not smart enough to be suspicious of a random so called prince emailing her out of anyone else to assist with an already questionable proposition. Today's scams are even more deceptive and complex.

There are a few different types of threats you need to be on the watch for. The first threat is the straight forward confidence trick, like what we just talked about. The second type of threat, phishing, is similar. Phishing is where information is gathered though subterfuge to run a separate attack. This could be to collect personal information or passwords. There are different terms you may hear related to this: Phishing is a trap sent to an indiscriminant list of targets; spear phishing is a purposeful trap sent to a specific target such as the accounting department of a single company; Whaling is a trap sent to executives of a company.

The third threat is payload attacks, where a virus or malware is installed. This can be to extort money or information, and can be delivered by fake emails with links or attachments, downloads, or even just looking at websites.

Vishing are phone call scams. There are several threat actors out there now that will call you directly and run some sort of line that they are with Microsoft or the FBI, or another company and they will

want information or access to your computer saying there is a virus or even pornography on your system.

It is imperative to have good and up to date end point protection. It can be from any of the top brand name companies, just as long as you have something. It is a common misconception that Apple computers, phones and tablets are not susceptible to virus. This is no longer true. While viruses and malware are more prevalent in Microsoft based operating systems, as Apple's market share and the use of portable devices grows, the more of a target they have become.

And while it should be an obvious statement, never send financial or personal information via email in response to a request. Banks will never ask you for personal information via email. Nor will the IRS or any government agency for that matter. They just won't do it. It will be in a formal manner most likely by postal mail.

Vigilance also includes things like making sure your computer, antivirus and applications are up to date with security patches, definitions, and updates. The Equifax breach of 2017 was solely due to two updates not being installed on one server for over a three month period. It was that simple. Those two simple, free updates cost 146 million users' their information and the jobs of a CIO, CISO and CEO.

It is just as important to be cognizant of how you dispose of hardware as you would give to protecting live data. Devices such as thumb drives, old computers, cell phones you are trading in, even copiers you have leased may have data on them. Special care may need to be given to sanitize these mediums to prevent data leakage.

Everything is a threat

The reason for our eternal vigilance is the last leg of SAVE.

Everything is a threat.

Everything is a vector.

Let's explore with a couple of anecdotes demonstrating what we mean by everything.

Our firm was called in to respond to a client reporting that they were unable to access any data on the server. We quickly determined that their server had been infected with ransomware. The first step to dealing with ransomware is find patient zero and remove it from the network. Step two, repair the damage. Due to the extent of the damage and the state of their backups, the client was down for 3 days while we cleaned and restored. Once they were running again, we started step three, the forensics.

It was determined from the evidence we found on the first infected computer that during the employee's lunch break, he was viewing a legitimate newspaper's website, a local paper from his home town, and was reading an article on a rookie football recruit. The newspaper had a link to the recruit's training films on YouTube. While the link did open the video, imbedded in that link was also a ransomware executable. And so the infection began. He was on his own time, reading a sports article in on a main stream news source.

The hackers had compromised the website and inserted a secondary command into the YouTube link so that it not only opened the video, it also ran a second instruction that downloaded and installed the ransomware.

In another incident we responded to, and while this may sound cliché, we assisted a large firm that was fallen by a VP looking at cat videos on Facebook.

If you were in a crowed restaurant and, rather than take your credit card and run it the waiter asks you to shout out the number across the floor so he could type it into the register, would you? You wouldn't, we hope, because you are in a public space surrounded by strangers. That's public Wi-Fi. Let's do another scenario. Let's say you go to a café, a Starbucks, you open your laptop, log in, open your email, and you see the same 5 emails we mentioned at the top of this discussion. Where is the threat this time? It was the moment you connected you to the Wi-Fi before you even accessed your email.

There are devices such as one called "The Pineapple" that only costs about $250 and are relatively easy to use. When you boot up your laptop, the first thing it tries to do is connect to known wireless access points. Your home, work, where ever you have saved. It calls out and says "Home? Are you there?" What the Pineapple does is say "Here I am" no matter what access point your computer asks for and unknowingly you are now connected. But what makes this even cleverer is, the Pineapple is also connected to the real Internet as well. So when you go to browse your Facebook, it lets you for the price of watching everything you type.

There is also a free program called Burp Suite. It works similar to the Pineapple, except, its specialty is mimicking websites. Facebook, Gmail, your bank, your company email page. All a hacker has to do is show it the real login screen. It copies the page, then displays it to a victim and who diligently provides their login name and password. It records what is typed then displays a very common 'wrong name or password'.

So not only did it get the login name and password, what do we normally do when we see a 'bad name or password' response? We try again. We try different passwords. It's human nature, a modern day call and response that we have been trained to follow. But now, not only did we provide the correct login initially, we've also probably gave a list of our commonly used passwords as well. Again, reiterating our earlier point, you should use different passwords for all sites.

We're not telling you all of this to show off clever "makes for good TV" tricks. We're demonstrating these very available and easy to use tools to emphasize how real and how accessible these concepts and threats are. It is not something that just happens in the movies or TV, and these days, you don't have to be a super hacker to do it. The tools practically do the job for you with a few clicks. It is not unreasonable to say the significant portion of the demographic using these are in fact teenagers and college age kids, what we call script kiddies.

There are things you can do to protect yourself. As previously mentioned, end point protection is the first step and the better quality ones not only have antivirus and malware protection but also a personal firewall to watch for break-ins. Second, you should always use a mobile hot spot rather than public Wi-Fi. Devices like the "MyFi" or "Jet Packs", or, most modern cell phones can be turned into a hotspot as well. Of course check your data plan.

This does bring us back to the discussion of convenience vs security. It takes extra effort to hook up the device, set it up, connect to it and so forth. But again, look at your risks. Is connecting too much effort, or is it more effort to deal with the fallout of your data being stolen, or your company and clients being breached. Try explaining to your client that you lost their data when your company login was taken because it was too much of a hassle to turn on your hot spot and connect.

For businesses, it is highly recommend having your IT department or provider set up a VPN service for your network, at a minimum. There are more complex, more secure systems that can be implemented like remote sessions in which all of the work you perform is within the safety of your corporate network rather than on your exposed laptop. But at a minimum, your network should incorporate a VPN solution. What a VPN does, is, setup a tunnel between your computer and the office network through the Internet. It's like a force field surrounding your data so you can talk securely. Imagine if just you and a colleague were talking in public and you didn't want anyone to hear the conversation so you surround yourselves with a tunnel of white noise machines. The two of you would then talk, but everyone else would hear static. That's what a VPN does for your data. Configured and used properly, this will thwart those previously mentioned hacker tools.

There is another part of cyber security awareness you should be aware of that doesn't necessarily use technology. That is social engineering. Social engineering is the use manipulation or observation of any aspect of a person's life to infer private information.

There is a TV show called Mr. Robot, about a hacktivist that gives a brilliant example of social engineering. The main character calls up a target on the phone and says 'mr.so and so, I'm with the credit card company and unfortunately there's been a breach on your account. Before we go any further, I need to confirm your identity. Are you still at such and such address?' The man reads back his address. 'Good. And what's your favorite sports team?' Yankees. 'And your pets names?' Flipper. By this time the target gets suspicious. The character hangs up and correctly says to the camera, with just this information and a brute force password cracker it will only take me a few hours to break into his account.

While this is a very accurate depiction of practical application, it doesn't have to be that dramatic or blatant to occur. Our team was at a hacker conference recently and was discussing this very topic. To demonstrate, we started chatting with our waitress. By the end of the conversation, we knew she was born in that town, her favorite sports team, her children's name, the name of her the baby she was expecting, her husband's name, what he did for a living, her pets' name and the name of her favorite pet from growing up.

Use of spouse, children, sports, pets or hobby is probably the number one most common characteristic of our population's password selection. How many secret questions use one of the things we learned from the waitress? Or how hard it would have been to determine her home address from online public records to pair with the rest of the information? Ironically, she knew there was a hacker conference going on in area and even said, "We all turn off our cell phones when they're in town because they broke in to some last year".

Now in this case, we are the good guys, so there was no harm done. But she was aware there was a threat and yet still openly provided that information. She was not vigilante and she did not assume everything is a threat. You could also say she didn't segment her personal life from her work life. We can say she did try to authenticate because she did ask what we were in town for but we said a pet food convention.

There are other aspects to social engineering you should keep in mind that don't evolve anyone even talking to you. Be aware of your surroundings. If you are on an airplane, know the person behind you can see what you are working on. On a flight someone might look between the airplane seats and see the person in front of them working on a pitch for a business loan. That's good intelligence for both a competitor and a hacker. This is particularly true if you are on a flight to a conference as many of the passengers may be as well and in the same line of business. Same goes for talking business on the phone or with colleagues in areas like a coffee shop or at the airport.

Let's take a look at company badges. Most are pretty innocuous. Maybe it just has a picture and name. How many pieces of information can you learn from a badge with only a name and a picture? With just that, at least 7 easy to get data points. Enough to start attacking a person's work account.

1. Your name
2. Your company name
3. What the company does and therefore what information they would have access to
4. Your job function and subsequently the type of data you would have access to
5. Your email address
6. You user name
7. And, it in itself, what your company ID badges look like

All of that from standing in line next to you at the lunch counter in only 10 seconds of glancing at the badge. Here's how:

First, obviously, there is your name. That's the biggest crack in the wall.

Next, where do we wear our badges the most? At or near our work. How many of you walk out of your building to lunch wearing your badge and go within a couple blocks radius of your office. If bad actor sitting at a restaurant or bar by an office building and more than one person comes in wearing the same badge then they would know it's related to a company within the vicinity. A walk around for a bit to see what buildings these style badges are coming out of, or, much easier, by just strike up a conversation with you such as "what business are you in? Oh, I have a need for that business, may I have your card?" would confirm this for them.

So now we know the name of a business, which a quick Internet search will then tell us what the business does and therefor what information they have. Are they a financial firm? Then they have a treasure trove of PII.

How many companies have their staff on the corporate website under the “Who we are” or “Our staff”? How many of persons have LinkedIn accounts? If a threat knows your name and where you work then they will most likely be able to see what your job function is which tells what information your network account will have access to. Are you a personal financial advisor? Then that account may have access to Social Security Numbers. Are you a CEO of a small to medium business? Then that account may have access to everything and an easy password.

Now we know your name, your business, what information your company may have, what information you may have access to. This is where it all starts coming together. Despite the fact that most likely we can find an email address with that information and a quick Internet search, most email addresses are first initial last name, or first name underscore or period last name or some such derivation. It only takes one test email trying all of the combos to see which one does not bounce back.

But here’s a real prize. Think of your email address. Now think of the user name you use to log into your company network or your email account. How similar are they? If not the exact same, probably pretty close enough to be worked out in a few tries.

So now we have a login name and a target. All that is needed now is a door with a lock to pick. And that is where our love hate relationship with convenience comes back into play yet again. How many of you use a web browser to access your company email? That door is available to anyone in the world to knock on.

And of course, the issue with the badge itself is, in this day and age with Photoshop like tools, it takes minimal effort to create a counterfeit badge affording a threat actor the ability to hang out at nearby local pub or in the building cafeteria to strike up a conversation, or roam the public areas collecting information, or maybe even get a friendly person to help hold the door open because their hands were full of empty boxes. If a company is a large company with many employees no one bats an eye at a new face.

Mind you, all of this is mitigated simply by tucking your badge behind your shirt or in your purse or pocket whenever you leave your office space. A simple five second action of vigilance most don’t even consider.

Our point to all of this is not to scare you into moving into a cabin in Montana with no electricity and wearing a tin foil hat. Rather, to give you a cautionary tale to encourage you to make the extra effort that’s absolutely necessary in this digital age to maintain some degree of safety to protect your, your business, or your client’s data, personal information, or even identity. You can never be 100% safe. You may get mugged walking down the street, but, that doesn’t stop you from leaving your home, you just take the precautions like only walking in safe areas and keeping your wits about you. The Internet is the same. As long as you follow these best practice tips as well as other means of mitigation, you can live and work in a relatively safe and productive environment.

If you would like further information, or assistance with implementing any of these suggestions, please do not hesitate to contact K_Street Consulting for professional, certified, cyber security service.