It is hard to even imagine a world without computers or the internet. In the past 25 years, automation and process simplification through technological advancements and remote connectivity between individuals and machines – and even between machines and other machines – by industrial controls has become commonplace in nearly every industry. Unfortunately, during the push for rapid innovation, dedicated to improving business processes, many cybersecurity vulnerabilities were, and are still, overlooked or simply undiscovered. The use of cybersecurity measures as an afterthought is certainly not optimal, but it was the hand we were dealt. Patching exploitable flaws in software code or deploying a wide array of cybersecurity appliances and applications may mitigate threats to some extent, but it is certainly not the total solution.

Good cybersecurity practitioners follow the principal of the C.I.A. Triad. No, we are not talking about the federal agency, although they should follow it as well. Rather, it’s an acronym that stands for Confidentiality, Integrity, and Availability. The goal is to keep confidential information out of the hands of unauthorized individuals, while protecting data integrity by ensuring that all information received, maintained, or transmitted via your systems is accurate and untampered with — all while allowing authorized individuals access to the data they are lawfully privy to. This creates some challenges. The best security is no one having access to anything, but that is not realistic. The key is to have a good balance between security and availability. The gap between the two is generally only protected by the vigilance of educated, but often non-technical individuals, who serve as your organization’s frontline guardians from the dangers on the information super highway.

With regards to determining the most critical component of a comprehensive cybersecurity program, the most detailed policies, robust plans, and advanced technological cybersecurity controls pale, in comparison, to the knowledge and practices of an end user. Yes, you, the end user — an individual who may have extremely limited technical understanding or capabilities with information technology — are the most crucial cybersecurity component. An uninformed system user is the softest of targets, and the path of least resistance for those who intend to do harm to an individual or organization via cyberspace. Unfortunately, in almost every major cyber-crime or cyber-terrorism event, some unaware employee or contractor unknowingly gave the attacker the keys to the proverbial kingdom.

Your attentiveness is paramount to protecting your organization’s critical data and systems. You are both the first and last line of defense against a cyber-threat. You must practice strong password safety. This limits outside attackers’ capability from gaining unlawful access. You must be aware of what a social engineering attack looks like. You should never trust anyone who asks you to do something that makes you uncomfortable. The primary modus operandi of a good social engineer is to establish a level of confidence with you so you feel comfortable enough to give them access to something that you
Social engineers are not simple tricksters, but masters of a sophisticated framework, with a vast toolkit at their disposal.

IDENTIFYING RISKS
For a risk to exist, three variables must be present:

1. You must have a target, which nearly every organization is.
2. The target must have a threat. This is simply someone with the desire to do harm.
3. The target must have at least one vulnerability that a threat can exploit. Uninformed people are always the biggest vulnerability.

It probably goes without saying, but the most common risk in most organizations is unauthorized access to critical systems and information. Some of the greatest tactics that criminals/terrorists use to attempt to gain access to your systems are social engineering, shoulder surfing, and phishing scams.

PASSWORD SAFETY
◆ Use strong passwords: at least eight characters long with uppercase and lowercase letters; include special characters and numbers; and do not use dictionary words. Make passwords easy for you to remember, but hard for someone to guess or for a cracking program to figure out.

◆ Never give your passwords to anyone (not even IT).

◆ Do not write your passwords anywhere. Instead, use an encrypted password manager so you only have to remember one password (the one to get into your password manager). There are several, and many are free. Some even have biometric-scanning capability.

◆ Do not use the same password for multiple systems or accounts.

◆ Use multifactor authentication where possible. For instance, if you use any device – other than your primary device – to access a system, after you put in your password, it will send a text to your phone with an authentication code to enter. You could also use token authentication like RSA.

SOCIAL ENGINEERING ATTACKS
Social engineering is the art of gaining access by manipulating a person into believing that they (the social engineer) are authorized, or getting you to allow them access, even if you know you shouldn’t. The latter being usually the work of someone skilled in the trade of spy-craft. Social engineers are not simple tricksters, but masters of a sophisticated framework, with a vast toolkit at their disposal. You can be a target of a social engineering scheme either in person, by email (phishing), through a fake website (pharming), or over the phone (vishing). It can range from something as simple as someone saying they are “from your internet service provider and they are there to fix some bandwidth issues on your network,” all the way to bribes, threats, blackmail, and even kidnapping of a loved-one to get you to do what they want.

The following are some tips to help you identify a social engineering attack:

◆ **The IT Helpdesk does not call end users.** In most modern organizations, technology specialists can fix IT issues without your help. They have administrative rights and will never ask you for your password. This includes software companies. Microsoft® will never call about a problem with your computer. Beware of anyone attempting to try to get you to provide any personal information, your password, or trying to get you to click on any unknown links, which are likely malware.

◆ **Beware of anyone attempting to over-escalate a sense of urgency** for something not normally an urgent matter. Some behaviors social engineers may try to create an environment that makes you feel as though you need to rush your thought process and overlook proper procedures. Tactics include sighing or sounds of disgust and continually looking at their watch or their phone. They may even have someone on the outside pretending to be their supervisor, or even a manager in your organization, sending them text messages, which they may show you, saying things such as, “what is the hold up?” etc.

◆ **Beware of threats,** even if they are minor and may not be perceived as a threat, such as someone saying, “(the boss) sent me to get this, and you definitely don’t want to make (the boss) have to come down here,” etc. Be extremely suspicious of anyone who tries to keep you from actually calling (the boss). They may say something such as, “I will just call him right now.”

◆ **Beware of anyone asking for access to anything, who makes an unscheduled visit.** Legitimate vendors will normally would not have awarded access. Remember: No matter how good your technical cybersecurity controls are, there will always be some malicious email traffic or websites that make it past the firewalls and spam filters. This is where you come in. You must not fall prey to this trickery, but be readily able to identify it and take the appropriate actions. Several studies have shown that educating employees on cybersecurity vulnerabilities, threats, risks, trends, and actions to mitigate issues will significantly improve your organization’s cybersecurity posture.

The following basic fundamentals should be included in every organization’s cybersecurity awareness program:

For a risk to exist, three variables must be present:

1. You must have a target, which nearly every organization is.
2. The target must have a threat. This is simply someone with the desire to do harm.
3. The target must have at least one vulnerability that a threat can exploit. Uninformed people are always the biggest vulnerability.

It probably goes without saying, but the most common risk in most organizations is unauthorized access to critical systems and information. Some of the greatest tactics that criminals/terrorists use to attempt to gain access to your systems are social engineering, shoulder surfing, and phishing scams.

Password Safety

- **Use strong passwords:** at least eight characters long with uppercase and lowercase letters; include special characters and numbers; and do not use dictionary words. Make passwords easy for you to remember, but hard for someone to guess or for a cracking program to figure out.

- **Never give your passwords to anyone (not even IT).**

- **Do not write your passwords anywhere.** Instead, use an encrypted password manager so you only have to remember one password (the one to get into your password manager). There are several, and many are free. Some even have biometric-scanning capability.

- **Do not use the same password for multiple systems or accounts.**

- **Use multifactor authentication where possible.** For instance, if you use any device – other than your primary device – to access a system, after you put in your password, it will send a text to your phone with an authentication code to enter. You could also use token authentication like RSA.

Social Engineering Attacks

Social engineering is the art of gaining access by manipulating a person into believing that they (the social engineer) are authorized, or getting you to allow them access, even if you know you shouldn’t. The latter being usually the work of someone skilled in the trade of spy-craft. Social engineers are not simple tricksters, but masters of a sophisticated framework, with a vast toolkit at their disposal. You can be a target of a social engineering scheme either in person, by email (phishing), through a fake website (pharming), or over the phone (vishing). It can range from something as simple as someone saying they are “from your internet service provider and they are there to fix some bandwidth issues on your network,” all the way to bribes, threats, blackmail, and even kidnapping of a loved-one to get you to do what they want.

The following are some tips to help you identify a social engineering attack:

- **The IT Helpdesk does not call end users.** In most modern organizations, technology specialists can fix IT issues without your help. They have administrative rights and will never ask you for your password. This includes software companies. Microsoft® will never call about a problem with your computer. Beware of anyone attempting to try to get you to provide any personal information, your password, or trying to get you to click on any unknown links, which are likely malware.

- **Beware of anyone attempting to over-escalate a sense of urgency** for something not normally an urgent matter. Some behaviors social engineers may try to create an environment that makes you feel as though you need to rush your thought process and overlook proper procedures. Tactics include sighing or sounds of disgust and continually looking at their watch or their phone. They may even have someone on the outside pretending to be their supervisor, or even a manager in your organization, sending them text messages, which they may show you, saying things such as, “what is the hold up?” etc.

- **Beware of threats,** even if they are minor and may not be perceived as a threat, such as someone saying, “(the boss) sent me to get this, and you definitely don’t want to make (the boss) have to come down here,” etc. Be extremely suspicious of anyone who tries to keep you from actually calling (the boss). They may say something such as, “I will just call him right now.”

- **Beware of anyone asking for access to anything, who makes an unscheduled visit.** Legitimate vendors will normally would not have awarded access. Remember: No matter how good your technical cybersecurity controls are, there will always be some malicious email traffic or websites that make it past the firewalls and spam filters. This is where you come in. You must not fall prey to this trickery, but be readily able to identify it and take the appropriate actions. Several studies have shown that educating employees on cybersecurity vulnerabilities, threats, risks, trends, and actions to mitigate issues will significantly improve your organization’s cybersecurity posture.

The following basic fundamentals should be included in every organization’s cybersecurity awareness program:

For a risk to exist, three variables must be present:

1. You must have a target, which nearly every organization is.
2. The target must have a threat. This is simply someone with the desire to do harm.
3. The target must have at least one vulnerability that a threat can exploit. Uninformed people are always the biggest vulnerability.

It probably goes without saying, but the most common risk in most organizations is unauthorized access to critical systems and information. Some of the greatest tactics that criminals/terrorists use to attempt to gain access to your systems are social engineering, shoulder surfing, and phishing scams.

Password Safety

- **Use strong passwords:** at least eight characters long with uppercase and lowercase letters; include special characters and numbers; and do not use dictionary words. Make passwords easy for you to remember, but hard for someone to guess or for a cracking program to figure out.

- **Never give your passwords to anyone (not even IT).**

- **Do not write your passwords anywhere.** Instead, use an encrypted password manager so you only have to remember one password (the one to get into your password manager). There are several, and many are free. Some even have biometric-scanning capability.

- **Do not use the same password for multiple systems or accounts.**

- **Use multifactor authentication where possible.** For instance, if you use any device – other than your primary device – to access a system, after you put in your password, it will send a text to your phone with an authentication code to enter. You could also use token authentication like RSA.
schedule appointments with the proper individual. Even inspections or audits should be coordinated through proper channels. If someone shows up saying they are there for an audit or inspection, thoroughly look over their credentials. Then, use a well-known search engine to find their website, call the office, and ask to speak to whoever is in charge of audits and/or inspections. Ask the legitimate person on the phone to verify the credentials of the auditors/inspectors before granting any access. All access to any facility or system should be monitored by a knowledgeable escort at all times. No unfettered access should ever be given to anyone.

♦ Beware of name droppers. Another common social engineering tactic is to drop the name of employees who usually are not at work that day. If you have the personal contact information for the employees whose names were dropped, do not hesitate to call them for verification.

♦ Always ask several questions. If you feel uncomfortable, bring in another colleague or, better yet, a senior manager. The more resistance that the social engineers receive the more likely they are to leave before they get caught. A person with legitimate business will generally wait until they receive the access they require. They have nothing to fear, if they are doing no wrong.

Another tactic that social engineers use is to try to get you to plug something into your system by saying something such as, “I need you to plug this into a USB port on your computer so I can run a quick diagnostic test to see if I can find the problem.” Or, they will simply leave flash drives laying in the lobby or in the employee parking lot. Never plug anything into your system that you find or an unknown individual hands to you. These will certainly contain malicious software.

SHOULDER SURFING
Shoulder surfing is when someone attempts to gain access to information they are not authorized to see by watching authorized individuals’ screens and keystrokes. This may be done covertly or overtly. Covert activity may take place over a sustained period of time, much like collecting small pieces of a large puzzle.

To protect against this, use screen protectors, which make it so only the user sitting directly in front of the screen can see the screen’s contents. Also, be aware of your surroundings and any suspicious behavior, such as someone trying to have a conversation with you where they have plain view of your screen. In this case, simply lock your screen while engaged in conversation. And, definitely lock your screen and secure any personal or confidential information from your desk any time you are away, even if just for a moment.

If your office faces a window or hallway, arrange your office space so your computer screen and any documents on your desk cannot be seen by anyone through the window or in the hallway. If you cannot arrange your desk, be sure to close your blinds when working with sensitive information. If you do not have blinds, request them or mirrored window tint, and use a screen protector.

PHISHING (EMAIL) & PHARMING (WEBSITES) ATTACKS
Phishing is like social engineering by email, except phishers use fraudulent copies or likenesses of familiar emails or websites, to get you to either click on a malicious link or transmit personal or otherwise sensitive information.

Pharming is when your browsing session is simply redirected to a fraudulent website that requests information, such as a fake bank login screen. Whether phished or pharmed, these forged copies of legitimate sites or emails are often so good even a well-trained professional cannot spot the errors.

The following tips should help you to identify and respond to a phishing attack:

♦ First, you need to determine whether the email you received is even genuine. Often times, the display name may be correct. However, if you hover your cursor/arrow over the display name or (with some email service providers you may have to right click on the name), you can see the sender’s actual email address. Most of the time, it is very obvious that the address is not correct, but occasionally you will have to pay special attention to detail. During a targeted phishing attack, the phisher may have created an email that looks very similar to the correct one, but may have used a dash or period, or even a one or capital “I” instead of a lowercase “i.” They look the same in many fonts.

If the email address is not real, anything contained in it is likely not real as well. Do not click on anything contained in the email or reply to the email. Block the sender or flag it as spam. Then, delete the email and empty your trash folder.

♦ When you receive a presumed legitimate email with a link to a website that also looks legitimate, do not click on the link. Instead, type the known URL to the website, or search for it on a well-known search engine. Certainly, beware of emails that just have a link to some URL you have never heard of.

♦ If you happen to click a link that you are unsure of and it takes you to a website, look for the “S.” Most legitimate business websites use secure URLs that start with “https://” and have the word “secure” or show a picture of a locked padlock in the address bar if the site is known to be secure. It is good practice to always look for this. However, a site without an “S” can still be secure. This is sometimes the case if the site’s Security Certificate has expired or it is registered to a different URL. You see this a lot with government sites or small businesses. Nevertheless, if the “S” is not there, proceed with caution.

♦ Look for spelling and grammar errors. An organization that spends good money on their webpage will generally attempt to ensure there are no spelling or grammatical
errors. Also, many hackers who create these phishing sites and emails are from outside the United States and do not possess a command of English, so they may use programs like Google Translate to convert it from their native language to English. This leads to often easy-to-identify errors. In many cases, the errors are purposefully there to try to circumvent cybersecurity controls such as spam filters, which block traffic based on certain key words.

As with telephone and/or in-person social engineering, phishers use similar language to instill a sense of urgency. Beware of statements such as, “failure to confirm your records may result in your account suspension,” or “due to security concerns...” Statements like these are almost always bogus. Real businesses will not send you threatening or urgent-sounding messages. Even your bank, if you missed a loan payment, will likely send you an email that reads something like, “We noticed you missed a payment on account ****1234. If there is anything we can do to help you make payment arrangements, please contact us at 1(800) ####### at your earliest convenience.”

◆ **Beware of important names.** Unless you are friends or already engaged in business with someone, it is doubtful any high-level official of any federal agency or Fortune 500 company will send you an email requesting urgent information.

◆ **Look for generic greetings and signature lines** such as, “Greetings valued customer” and signed by “…Service Representative.” This is usually the case when the phishing scam has been sent as a bulk email blast and is not a targeted phishing attack.

◆ **Beware of low-resolution graphics.** This is almost always a tell-tale sign something is wrong.

◆ **Never click on attachments from an unknown sender** or when the attachments are in an unsolicited email. These can contain malware.

Now that you know most of the signs and actions, you should go to:

https://opendns.com/phishing-quiz/

to test your knowledge on a Phishing Quiz. This is a link you should never be afraid of. In fact, share it with your organization so others can become more aware.

**TAB NABBING**

This is when a hacker hijacks a tab on your browser. When a hacker sees that you have multiple tabs open in your browser, and one of them has not been accessed recently, the hacker will take control of that tab and change it to a spoof site to try to get information from you. The most common trend is to change the tab to a page that looks like your email login screen and that indicates your session has expired and you need to log back in. Always type the site’s URL into the address bar. For instance, if you see a tab that indicates you were logged out of a social media site, rather than logging back in there, simply close the tab, open a new one and type the social media site’s known URL into the address bar to log back in.

**WHAT ELSE CAN I DO?**

In addition to the knowledge you have gained, you can take several steps to get in front of a cyber-attack. At a minimum, if you do not have an IT department or person on staff, you should. But if you don’t, make sure your operating systems and all software packages are up to date, you have a well-known antivirus software installed, and you run periodic scans for malware on your systems. There are several products, and many are free. If you do install antivirus software on your system, only install one product. These programs are built on databases of virus definitions. When you install more than one on the same system, they tend to attack one another.

**SECURE EMAIL AND INTELLIGENCE SHARING**

Is your organization using a secure encrypted email service? If not, IAMU has partnered with the Iowa Department of Public Safety, Fusion Center, and the U.S. Department of Justice to roll out RISS ATIX Accounts, free of charge, for all employees of member utilities who may have access to sensitive information not subject to public disclosure and is designated as “Confidential” under Iowa Code §22.7(50), for the protection of critical infrastructure. A brochure about RISS ATIX can be found at: https://www.riss.net/files/atix-brochure/. The goal is to have every utility in Iowa connected to the RISS-Net as part of a secure online information-sharing community. MidAmerican Energy and Alliant Energy have been using RISS ATIX for a while. It is time that the municipal utilities have the same protection. After identifying who in your utility should have an account, contact me at rsaffell@atix.riss.net, and I will get them set up.

If you have an account on the IAMU website, please visit the Member Security and Preparedness site at: www.iamu.org/security for more information. You will be asked to log in. If you do not have an account, contact webmaster@iamu.org to register for one.

Remember to share the information you have learned here with everyone you can. By spreading this knowledge, we will create a network of cyber guardians to serve on the front lines in the cyber war for Iowa’s critical utility infrastructure.

---

For more information and resources on security – both cyber and physical – both visit: www.iamu.org/security