Monthly Cybersecurity Newsletter

December 2018 Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

---

Don't Take the Bait!

According to Verizon's 2018 Data Breach Investigations Report, phishing or other forms of social engineering cause **93% of all data breaches!** For social engineering attacks to be successful, the attacker just needs a target to take the bait. *You are the target*, or to put it another way, the fish that bite. Email continues to be the main source of a data breach – 96% of cases. To make matters worse, a cybercriminal only needs **one victim** to get access into an organization. Organizations are much more likely to get breached by social attacks than through actual system vulnerabilities, emphasizing the need for ongoing employee cybersecurity awareness and training.

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. Phishing is a form of social engineering that uses email or malicious websites to solicit personal information by posing as a trustworthy source. For example, an attacker may send an email seemingly from a reputable source, such as a vendor or a colleague, that requests account information. The message will often suggest there is a problem and indicate a sense of urgency. If you respond to the message with the requested information, an attacker can then use it to gain access to your accounts. Attackers will also take advantage of current events, such as the following:

- Natural disasters (e.g., Hurricane Florence or Matthew)
- Epidemics and health scares (e.g., H1N1, food contamination)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

Implementing IT security controls such as strong passwords, firewalls, anti-virus protection and encryption, are only a **part** of the solution in reducing the risk of a cyberattack. In fact, if the Verizon report is correct, those security measures are not even the most important measures in protecting our data and resources. Training ourselves and our colleagues to recognize and to respond appropriately to cyber threats is of paramount importance to prevent these types of cyber attacks. We must become more aware of the risks associated with clicking on a link in a phishing email, downloading an attachment from an unknown sender, or responding to requests for personal information or other sensitive data.

How can you avoid being a victim?

The United States Computer Emergency Readiness Team (US-CERT) suggests the following tips to help you avoid becoming a victim to social engineering:

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking for internal information. Verify the identity of the person contacting you!
- Do not provide information about yourself or your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal sensitive information in email, and do not respond to email solicitations for this information. This includes clicking on links that are in an unsolicited email.
- Pay attention to the Uniform Resource Locator (URL) of a website. Malicious websites ***may look identical*** to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the sender directly. Do not use contact information that is provided in the message, though.

Be sure to check out the resources attached to the end of this newsletter: ***Why Phishing Works*** and ***A Cautionary Tale in Phishing***. Remember…*Cybersecurity is our shared responsibility* and you can be the strongest link in the cybersecurity chain. Don't take the bait!

Avoid Holiday Scams

It is that time of year again. We are finishing that last minute gift shopping and preparing for some time with family and friends. While the season should be a time of happiness and generosity, it can also be a stressful time when cybercriminals exploit others. The season is also a great time to make chartable gifts to support the causes you care about. Many charitable organizations run end-of-year fundraising campaigns. The sad thing is criminals know this and take advantage of people by running scams in an attempt to fool people into giving them money. The following are some common scams and some tips on how to avoid them.

- **Fake Charity Websites:** One of the most convincing ways for cybercriminals to exploit charitable giving is by creating convincing charity websites. These websites are in fact fraudulent and may copy an existing charity's site or use the charity's name and branding:
- ✓ Browse directly to the charity by entering the charity's URL into your browser's address bar.
- ✓ Carefully study the website's URL for typos. Fake sites can look very similar to the original.
- ✓ Research an organization's correct information by using the Federal Trade Commission's charity guide, or through resources like GuideStar, Charity Navigator, and Charity Watch.
- **Social Media Donation Pleas:** Scammers commonly impersonate staff from major charities via social media channels. Avoid making donations through social media and never send your personal or payment information in a social media message. Instead, consider heading directly to a charity's established website.

Lastly, when donating to a charity, make sure the charity is a registered charity under U.S. or international tax law. U.S. 501 charities have to make certain information public and you can find the charity and its information on any of the several charity tracking websites.

Don't forget the other **monthly newsletters** that are available to you. The following are some other cybersecurity newsletters the ESRMO recommends to you. We hope you find them beneficial.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month is on ***Security and Privacy in the Connected Home.***

- https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Yes, You Are a Target.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

---

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link: https://www.sans.org/webcasts/upcoming.

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at no cost to government staff, including contractors. With 60+ courses at varying levels of proficiency – from beginners to advanced – all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated on a rolling basis.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available courses of varying proficiency – beginner to advanced
- ✓ Self-paced
- ✓ Many popular certification courses
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework
- ✓ Taught by experienced cybersecurity subject matter experts

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

FEMA Emergency Management Institute Weekly EMI e-Forums are 1-hour, moderated, webinar discussion forums that provide an opportunity for EMI and the emergency management community to discuss matters of interest on national preparedness training. EMI e-Forums facilitate a discussion of whole community-presented best practices. These sessions are scheduled for Wednesdays in January from 3:00 p.m. to 4:00 p.m. EDT and they are free of charge and available to anyone who wishes to participate. For more information and a list of the upcoming sessions, please view the training bulletin.

Why Phishing Works

A successful phishing attack accomplishes two basic goals: ***it gains the trust of victims and exploits their emotions.*** Take, for example, those classic advance-fee scams that promise a large sum of money for a small up front payment. You would never fall for one of those, right? Of course not. They're incredibly easy to spot, thanks to their too-good-to-be-true nature. But other phishing scams are more advanced.

Imagine a friend of yours is looking for a job. She posts her resume on various sites and sends out applications. Then, she finally receives an email, that appears to come from Linkedin, with a great job offer. ***All your friend has to do is click the link and upload her personal details. But is it a scam?*** More importantly, would your friend, who has been on the job hunt for several months, even question its authenticity?

Now let's flip roles. Let's say you handle the hiring of new employees and you get lots of emails from applicants with attachments. ***How difficult would it be for a social engineer to push a malicious attachment, disguised as a resumé, to your inbox?***

What about emails that appear to come from someone you know? Let's say a friend sends you a message that he's traveling abroad, has been robbed, and urgently needs *you* to wire him money in order to buy a ticket home. How would you respond?

It is easy for social engineers to leverage emotions like compassion or concern against their targets. It gets even easier when their targets are at a point of desperation, often related to financial need.

Simply put, people fall for advance-fee scams. People fall for fake job offerings. People fall for threats that claim to come from tax collection agencies. ***Trust, desperation, and fear: the most effective weapons of scammers.***

Phishing Identification Checklist

- ☐ Does the email contain poor spelling and/or bad grammar?
- ☐ Is the email awkwardly worded or nonsensical?
- ☐ Is the "from" address unrecognizable or just plain weird?
- ☐ Does the email promise large sums of money or other unbelievable offers?
- ☐ Does the email use threatening language?
- ☐ Does the email contain a sense of urgency?
- ☐ Does the email have a call-to-action such as clicking a link?
- ☐ Does the email contain an unexpected attachment or request for money?

If you had to check any of these boxes, beware! You could be under attack!

As always, follow our organization's policies and report security incidents, such as potential phishing attacks, immediately. If you have any questions, please ask!

DID YOU KNOW...

Email addresses can be spoofed, or forged, to make messages appear to come from legitimate sources. Victims are much more likely to cooperate when they believe they are communicating with someone they know, which is even more reason to fully scrutinize all requests for sensitive info or money!

A Cautionary Tale in Phishing

The following account from a colleague details how easy it is to get phished. As you read it, just think about your day-to-day routine and ask yourself: would this ever happen to me?

I probably get about 150 emails a day. Sometimes more. If I were to guess, I'd say at least two or three of those are spam or phishing of some sort. Needless to say, I'm pretty good at spotting them.

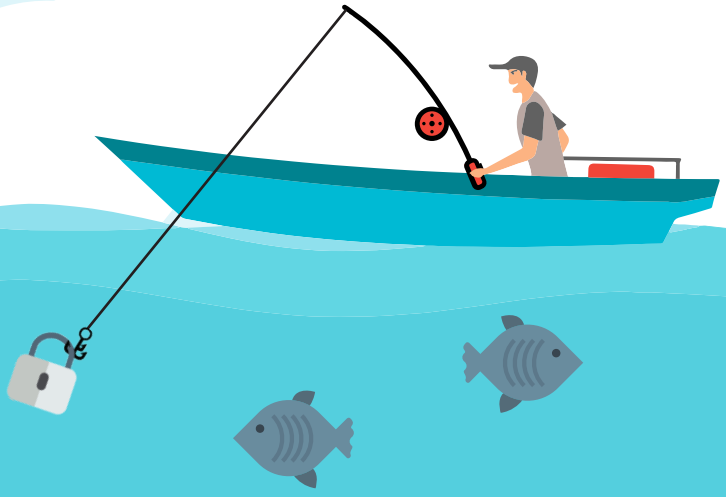
At least I thought I was.

It was one of those weeks when the perfect storm hit. We onboarded several new employees, plus added a few major client accounts. All good things, but incredibly busy. Just lots of paperwork.

So, late Friday afternoon after a long week, I was processing tax info for my new co-workers. Maybe I was working too fast, not being thorough enough. Hard to say. But I only had a few more to get through. I opened an email that I thought was from a new employee and downloaded the attached document—standard stuff.

But when I opened the document, it was blank. Confused, I went back to my email client to see if maybe it had messed up during the download. But before I could even get there, my antivirus suddenly popped up in the middle of the screen with an alert that it had detected a hostile threat. Five seconds later, my whole screen went black and was replaced by a **ransomware** note.

This victim's story illustrates an important lesson in cybersecurity: anyone can make a mistake, even the most cautious person. Busy work seasons and long weeks can lead to security awareness being a bit lax. But remember that all your hard work will be for naught if our networks are compromised by a phishing attack! Slow down, stay alert, and think before you click.



Ransomware Everywhere

According to a recent study, ransomware attacks have surged, with over 181 million attacks in the first six months of this year. For reference, that's a **229% increase** over the same time frame in 2017. Why does this matter to you? Because it shows that phishers have changed their bait. For years, their goal was to infect systems with malware and steal sensitive data. That still happens, but the market for selling sensitive data on the dark web has become oversaturated, thanks to multiple major data breaches.

Hence, scammers have adopted ransomware, which promises a much easier and quicker way to profit. Keep that in mind as you go about your daily routines. **One wrong click** could lock up our entire network!

High-Profile Ransomware Case

Early on a Thursday morning in March 2018, the City of Atlanta came under attack. A ransomware variant known as SamSam shut down five of the city's 13 local government departments, crippling their systems and knocking nearly a third of their programs offline. As hours and days passed, the attack prevented the city from collecting revenue. It left residents unable to pay utility bills or request services. It forced the police and other city departments to file paper reports, grinding operations to a halt.

In the end, the city's systems were offline for over a week, 6 million people were impacted, and the cost of recovery is expected to reach nearly nine million dollars.

This attack exemplifies the dangers of ransomware. And even though SamSam doesn't necessarily rely on phishing emails to infect systems *(it utilizes weak and stolen credentials to gain access to vulnerable servers)*, most other variants do, and their impacts present just as much of a threat. Once again, use common sense, slow down a bit, and think before you click!