Mike Galler

They're Phishing for You

Be the One That Got Away!

MIKE GALLER, MEMBER ASHRAE

Cybersecurity has been a topic of increasing importance to the building services community for several years. While fully securing large and complex building systems can be complicated, some basic precautions can easily be applied to any system, and some basic precautions can be implemented by the users of any system. This column will briefly explore an important aspect of cybersecurity that can affect both information technology (IT) and operational technology (OT) networks—a type of attack called phishing.

What is Phishing?

Phishing attacks are a type of social engineering attack where criminals attempt to obtain information from victims, or trick victims into giving the attackers access to their computers or networks. The information may be personal (i.e., financial, social security number) or business (i.e., business secrets, plans, data or passwords). If given access the attackers can then install malware on the victims' systems and use them for further attacks.

How Big a Problem is Phishing?

Phishing accounts for 90% of data breaches and is considered one of the top cybersecurity risks. Phishing attacks were reported by 83% of organizations.[1] The average cost to an organization to recover from a successful attack is over $4 million.[2]

Who is Targeted by Phishing?

Anyone can be the target of a phishing attack. Just as someone who is actually fishing would rarely target a specific fish when throwing out a line or a net, phishers will catch anyone they can when they are sending out most attacks, but there is no size limit for them. Targeted attacks, often called spear phishing or whaling, may be directed at an individual high value target such as a system administrator or C-level executive. Targeted attacks may be customized for the victim and are more difficult to spot. They are less common due to the additional effort required.

How is Phishing Done?

Phishing attacks may come in many forms, including e-mail, social media, phone or text message. The message or caller may claim to be from a bank, credit card or other financial institution. They may claim to urgently need your account number, credit card number, a

Mike Galler is an engineer at the National Institute of Standards and Technology in Gaithersburg, Md.

iSTOCK.COM/STEVANOVICIGOR

password or other information. They may claim that you have won a prize or are due a payment. They could be posing as a charity or political cause. They may say that they need the information to stop an imminent threat, such as hacking or a virus. They may claim to be someone high up in your organization who urgently needs sensitive information or access to a network, or they may pose as someone from your IT department or from a software vendor and ask for credentials to connect to your computer. Some attacks direct the victim to a website to enter information.

What the attackers lack in morals they make up for in creativity. It's important to realize that this is an attack against you and your company. If it's a targeted attack they may even have some accurate information, such as an account number, email address or a password. The information is probably out of date. Criminals sell information from previous data breaches to other criminals to use in their attacks.

Types of Phishing

Attackers can use multiple methods to contact a victim. Some of the more common types are:

- Email phishing—the most common type. An email is sent with a dire warning (you've been hacked!) or an extortion attempt where they claim to have compromising pictures or video of you (note: they do not). Business email compromise (BEC) attacks are a type of email phishing attack where a company executive or other representative is impersonated. They may claim a situation that requires urgency and demand that you take some action (clicking a link, sending them some information) immediately. Their demand probably violates company security policy as well as common sense. The false sense of urgency is to get you to panic and act before thinking.
- Smishing—an attack that uses text messaging or short message service (SMS) to execute the attack. A common smishing technique is to deliver a message to a cell phone through SMS that contains a clickable link or a return phone number.
- Vishing—term for when the attacker contacts the victim through a voice call.
- Spear phishing—targets a specific group or type of individual such as a company's system administrator.
- Whaling—an even more targeted type of phishing that goes after large "whales" instead of small fish, typically targeting a C-level executive.
- Search engine phishing—hackers become the top result in a search engine, masquerading as a legitimate website.
- Pharming—Internet traffic is routed to a fake website, which may have malware or may try to gather information. This may affect one person or large numbers of people. One dangerous aspect of this type of attack is that it can happen without any action being

taken by the user since the redirection takes place outside of their network.

How to Protect Yourself From Phishing

As with most aspects of security, protecting yourself from phishing requires a low level of constant vigilance. Methods to recognize phishing attempts should be included in company-provided cybersecurity training. Many phishing attacks are relatively easy to spot if you know what to look for. Clues that a message might be a phishing attack include:

- Misspellings, grammar, or punctuation errors. An email that purports to be official correspondence from a legitimate company should have none of these problems. Personal correspondence may not have this expectation.
- Uses generic email instead of a company email address. A message from an address such as YourCompanyCEO@gmail.com is very suspicious.
- False sense of urgency, possibly through a threat or expiring offer. They are trying to get you to act without thinking.
- Requests personal information, such as an account number, password or financial data. This type of information should never be legitimately requested by email.
- Be careful with attachments, links and remote content. Attackers may send an infected file or malware as an attachment. The name of the file may be designed to make you think it's safe when it's not ("PLEASE_OPEN.DOC.exe"). Links may also be designed to deceive. The text of the link may show the URL for one website but take you to another. You can check the actual destination by hovering your mouse cursor over the link. The actual destination will be shown in a pop-up window or at the bottom of the email application window. Some phishing attacks can be launched just by loading remote content, such as pictures in an email. If you don't trust the sender, then don't download attachments or load remote content.
- Uses a misspelled or unusual domain name, i.e., AHSRAE.org (note the swapped letters), or from an unusual Top Level Domain.

If you find any of these indicators in a message, take a minute and look for more. Many phishing attempts will be obvious if carefully examined. It is also important to check that your outgoing email does not exhibit any of these characteristics, so it is not mislabeled as spam or a phishing attack by the recipients.

Top Level Domains

The top level domain (TLD) is the last part of the website name. A few are widely used, such as .com, .org, .net, .edu, and .gov. There is also a TLD for every country, such as .us for the USA or .ca for Canada. There were 1,487[3] unique TLDs in use when this column was written.[3] It is unlikely that any company has registered their name in all of them. Criminals frequently register domain names anonymously and use those domains for phishing, distributing malware or other illegal activity. If an email is from or directs you to an address that looks suspicious, don't trust it. Following links to http://ASHRAE.VACATIONS will not lead to any relaxation.

What to Do if You Are Phished

Don't panic! Also, don't click on anything in the message, don't let your email viewer load remote content or pictures and don't download any attachments. If a message looks suspicious, forward it to your IT department if you have one and then delete it. Many companies have established IT procedures that you should follow above all other advice.

If you clicked on an attachment or link and think your computer has been infected, you should immediately contain the infection by disconnecting your computer from the network[4] and informing your IT department or specialist. If possible, put it in hibernation mode. Do not shut down the computer, as a virus or malware may have more opportunities to damage your system when it restarts.[5] Your IT specialists should have the knowledge and tools to inspect and clean your system safely.

References

1. CyberTalk.org. 2022. "Top 15 Phishing Attack Statistics (And They Might Scare You)." CyberTalk.org. https://tinyurl.com/bdwhj646

2. IBM. 2022. "Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond." IBM. https://tinyurl.com/yc5arrum

3. IANA. Undated. "TLDS Alpha by Domain." IANA. https://data.iana.org/TLD/tlds-alpha-by-domain.txt

4. NIST. 2013. "Guide to Malware Incident Prevention and Handling for Desktops and Laptops." NIST SP800-83 R1. National Institute of Standards and Technology.

5. Cimpanu, C. 2019. "Experts: Don't Reboot Your Computer After You've Been Infected With Ransomware." ZDNET.com. https://tinyurl.com/2p8byp64 ■