PHISHING EMAILS TO WATCH FOR

PHISHING EMAILS are a fact of life these days. Death, taxes, and phishing emails. Verizon's 2019 Data Breach Investigations Report lists phishing attacks and the use of stolen credentials (attained through phishing) as the top two sources of breaches in the financial and insurance sectors.[1]

These emails come in a wide variety of styles and techniques and attempt to accomplish a wide range of goals. Some are targeted and personal, while others are generic and sent out to hundreds of people at a time, hoping at least a couple will fall into the trap. Some are trying to pry a little bit of useful information; others are trying to get into the system by acquiring credentials or installing malicious software attached to the phishing email.

Robust security systems are a huge asset in blocking these emails, but some will inevitably make it through to employees. Therefore, it's vital for employees to be well trained in what to look for in potential malicious emails.

Start with the sender. Who did this email come from? Was I expecting an email from this person? Does the cadence seem familiar based on prior communication?

At first glance, the name at the bottom of the email might be a name you're familiar with. But did it actually come from that person? Look closely at the "From" address and the external sender warning. Some emails are less sophisticated than others. Example 1 is riddled with clues, but here are some of the highlights from top to bottom.

Example 1 - Quick Task

QUICK TASK

SH **Shawn A. Huff** <ipad@ipad09.net>
To mmeleedy@aimmutual.com

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Are you unoccupied at the moment to run an errand. I'm tied up right now.Reply if you're available.

Regards,

Shawn.

Sent from my iPad

"...IT'S VITAL FOR EMPLOYEES TO BE WELL TRAINED IN WHAT TO LOOK FOR IN POTENTIAL MALICIOUS EMAILS."

- The subject line is short, undescriptive, and in all capital letters. Is this normal for this sender?
- The sender name is the full first name, middle initial, and last name. Do this person's emails typically come through like this?
- The sending address is a glaring clue on this one. Is that the person's normal email address?
- This email contains an External Sender Warning, which is warning that this email originated from outside the company. If this were an internal communication, sent from this person's work email address, there should not be an external sender warning.
- There is no greeting in the body of the email and the request could be atypical for something this person would normally request of you. Also, the cadence of the request is abrupt and might not be typical of this sender.
- The email is signed Regards, followed by only the first name and a period. Is this how this person normally signs his emails?
- Lastly, the last line is "Sent from my iPad." This person might not typically send emails with an iPad warning at the bottom.

Any one of these signs by itself is cause to question the email, and the more signs, the more wary you should be.

Example 1 is more obvious than most. However, the most effective phishing emails look very convincing and come from people and companies that you know and have ties to.

The Next Level

It's especially important to be alert to any request for personal information, no matter how familiar you are with the sender or how urgent the request is. You might get an email like Example 2, telling you someone is trying to gain access to an account and you need to click a link to log in and reset your password or re-enable your account.

This can be scary when it's coming from a place like a bank, but that's the point. The attacker wants you to panic and make a rash decision to click an unverified link. Many companies send emails like this when unauthorized attempts are made to access accounts, but the valid ones will not ask you to click a link. They will simply suggest changing your password. This forces you to go to the actual website that you know is legitimate rather than clicking an unknown link.

Example 2 - Unknown Link

Dear Customer,

Several failed login attempts have been made to your account. For security purposes we have disabled your account until you can confirm your username and password.

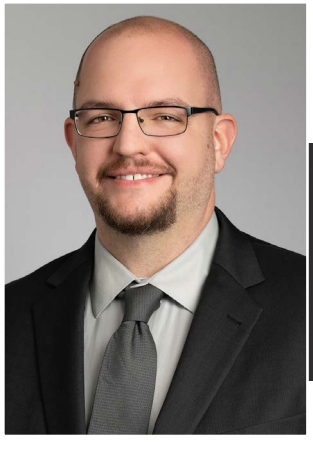
Please use the link below to log in and re-enable your account:
https://na1sfsecurity.com/secure/accountlockout.jsp?
r=oweihwoihc029jiwpicoscwCRAR34t4f_Wf4w4CAeORCMKSOECJwoejucowekac.a1g%3D%3D&display=page&fpot=c74cb
c125-4ad9-9000-73f427cb46ec08027ecf-62d3-4450-b576-215cbaf96526

If you have any questions, please contact the administrator for your company.

Thank you.

The best advice possible, when it comes to suspicious emails, is to slow down, scrutinize, and ask questions. Most companies have layers of protection in place such as endpoint protection, firewalls, multi-factor authentication, and email and web filtering, but one of the most effective layers of protection is a well-trained employee who knows what to look for.

[1]Verizon, 2019 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report-emea.pdf.



SHAWN HUFF is a Network Analyst for A.I.M. Mutual Insurance. He has been in IT for more than 10 years, working on security systems and projects such as managing firewalls, setting up and configuring email/web filters, rolling out multi-factor authentication, and configuring device management systems. He has worked in environments ranging from retail to higher education and insurance. Shawn holds an associate degree from Northern Essex Community College.