ONE PHISH, TWO PHISH

TIM'S THOUGHTS

timh@nhghotels.com

TLDR

TEACHING • LEARNING • DOING • REINFORCING

BY TIM HAYES
DIRECTOR OF
FINANCIAL ANALYSIS

Over the last year or longer, I have made it my mission to educate us, as an organization, on phishing. I have done so, and will continue to do so, by making examples of phishing emails and pointing out the signs that an email is illegitimate. I will always encourage all of you to share these practices with your team members, but also with your friend and family. Sadly, these phishing scams don't end at the workplace. Today, I'd like to go into detail about the end goal of the phisher and offer a better understanding of what these individuals gain from what they do.

In many of the cases we have seen recently, phishing emails aim to get the receiver to click a link within their email. They accomplish this through deploying several different tactics including pressuring the receiver through urgency, presenting themselves as someone the receiver know through a different email address, or by hiding the link behind an image or a spoofed "Unsubscribe" link. This link leads the receiver to a website that automatically extracts their Outlook password. Two factor authentication can block this, but the phisher can continuously attempt to access the account and flood you with access requests until you either grant them access or change your password. You should most certainly do the latter.

When the phisher gains access to your outlook, what they're after at this stage is your contact list and the legitimacy they gain when sending an email to everyone in your contacts from your email address. They will then attempt to use your email to phish other email accounts in your contacts to increase the number of legitimate emails they can phish with. Eventually, they use these emails to get someone in their contacts to buy gift card, request change someone's payroll banking information, or outright requests for money transfers. The phisher has a lot more options open to them when they're perceived to be someone who works for the company.

The best defense against this is not getting compromised to begin with. Enabling two-factor authentication on your email accounts is a great safeguard against getting to have your account compromised. Secondly, you should never authorize any two-factor authentication prompts unless you have physically attempted to sign in yourself. If you receive an email from an unknown sender, you should not click anything within the email, especially if the email is prompting you to act quickly.

Lastly, if you receive an email from someone you normally communicate with, but the email does not read like they usually communicate, call them, and ask about the email. If you get an attachment without any explanation, again, call the sender and ask out the email. And, of course, if you receive a request to buy gift cards or transfer money of any kind, call the sender and confirm. In all these cases, it's better to err on the side of caution and over communicate.

– TH