Science Translations
Established 1990
PC410.COM™
PC Updater News

Spear-Phish Hoaxes

A phish, again, is an email that looks tempting, but is bait for something else. It might have an attachment that's dangerous, maybe a fake invoice, summons, or gift card, leading to a program or script named to look like it's just a document. But sometimes, there is no attachment, and no link to click.

Businesses should expect to get spear-phish emails. These are more targeted, and may include actual names of people in your office, or might not. Tthe most common type asks for a price quote of something that your type of business might sell. In my case, I've seen them for 200 hard drives, 5 laptop computers, web design jobs, and for the "repair" of 15 computers. That last one came from a hotmail account with no company name, first warning flag.

The email was short. Basically unbelievable, not remotely how people buy those things. So I kept my reply short. "Yes, I can repair those, if you're local."

‘Laura’ sent back a list of work, not repairs at all, including: format the hard drive, install Windows and Office, cleaning, and so on. That’s routine for a big pile of notebooks for a computer refurbishment company, but not the kind of work I expect while working with local businesses to manage their technology. But OK, I quoted $320 per computer plus shipping, which is more than those computers are worth, so that I could see how the scam would work.

Laura’s next reply explained it:

Thanks for the mail, My Employer company just inform me few minutes ago from our head office that your payment has been ready but remain to be mail to your company address.

Mind you, a payment of $3750 [which is my salary and travel allowance last month] has been issue out in your name from my Employer company which you just need deduct your own payment out of the money and help us to send the remaining amount to our shipper coming from a nearby state to drop the computers and also to pick them up on completion.

Sorry for not inform you about this before, I guess things will work out as well.

Hope we can count on you about the payment and with my money and your service.

Hope to read from you soon.

Laura.

My reply basically said, “Sounds great...” and asking how many computers would be sent, but carefully failing to give my shipping address. Her reply, and the point where I just stopped answering:

Thanks for the mail .

I must confess I'm comfortable with the cost and its quite reasonable and affordable and also,i hope i can trust you that to do a good job.

I will be sending you the payment inform of US certified cashier check mailed and addressed to you and regards to this kindly get back to me with your full information (in the format below)to receive the payment so it can be made out on-time.

At this point, they want to pay in advance , and have me pay their courier out of the check they’re sending. There are no computers to repair. It’s just an attempt to have me cash a check, maybe counterfeit, or a real, valid check stolen from a US-based company, which would be paid by the bank and then caught by the

company and result in a visit from the FBI, demands for restitution, and potential jail time.

The phish emails vary, considerably, by industry. It will show up in your email as a potential order for a few thousand dollars of whatever you sell or create. The sender will have a free email account, and very little location information. They will, on reply, agree to any price, as long as they can pay you and have you pay their money mule.

What's a Money Mule?

In short, it's the other half of the scam, where someone has been given a job to pick up the cash, pay themselves out of it, and then send the rest overseas by money order number, without any paper to mail.

The FBI explains it well:
https://www.fbi.gov/news/stories/fbi-joins-international-campaign-to-stop-money-mules-121718

Variation 1: I've had a request from a fake "Deputy Chief Financial Officer at Nuclear Regulatory Commission" to please sell them 40 laptop computers, all high-end, and 100 backup drives, all to be delivered to Rockville MD, the real address of the NRC, but the email reply address was from a .US domain, not .GOV, and the phone number had an area code only used for cell phones. That's not how the US Government bid process works. That email arrived from an online vendor of combat uniforms, who probably didn't know that they had lost control of their email accounts.

Variation 2: One scam attempt sent three consecutively-numbered credit card accounts to split payment for an order, with a billing address in Florida, "please ship these to Louisiana and Alabama." I looked up the first four digits of the card, and called the issuer, NationsBank. Their fraud department said, "That would have passed authorization, but those accounts aren't the same person. Without a written signature, there would have been a chargeback. Thank you so much for calling us."

Every reader of this newsletter is too smart to hand cash to a courier, or split a shipped order over multiple credit cards. But just replying to these scams is a major waste of time, especially investing time in quote creation.

Finally, sometimes the scammers send the wrong email. For the record, I am not a lawyer. I am a tech, in Maryland, not Iowa, and not Tennessee. This is from last week:

"Hi Jerry: We have a local buyer in your state (Shawver Well Company

Fredericksburg, IA 50630) who is interested in purchasing our Drillmec HH-300 Oil Rig currently located at the port of Chattanooga Tennessee and we need an attorney that would draft a purchase and sales agreement for this transaction. I have attached the Spec-Sheet of the Rig for your review. If you can handle this please email to me your engagement letter as well as your rate and retainer fee."

Sure, I'll get right on that.

Phish Training: Infographic

Here's a handout for your staff, telling what's wrong with a sample phish. It's a single-page, ready for employee training.

https://pc410.com/download/DontClickThatPhish_infographic.pdf

---

Windows 1909 Arrives

The newest semi-annual update for Windows 10 will be available very soon, and this one will be numbered as '1909', as always, that's for the year and month. The update is not the usual feature update this time.

Previous feature updates were big things, lengthy installs requiring hour-long reboots and a full download of the operating system. Starting with this update, the second big update of each year will contain a catch-up package of patches since the last feature update, have very few new features, and will install as a normal patch, with a short reboot. That's if your computer is updating from the Spring version, known this time as '1903'. From earlier versions, the lengthy reinstall with an hour-long reboot will still happen this time.

As always, to identify the installed version of Windows, click on Start, also known as the white Windows logo, type 'winv' and click on 'WinVer' in the search results.

As of November 12th, 2019, Windows version 1803 and older will no longer receive patches, and no longer be in compliance with some government and financial requirements, so the results in WinVer should be 1809 (2018 September) or newer. And Windows 7 reaches the same state of non-compliance on January 14th, 2020. Call if you need help updating a computer.

For computer help, call 410-871-2877