Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

Phish Tales

Some of my email addresses have been online since 1992, and are easy to look up, so I get scam attempts mixed into spam fairly regularly. Here are some newer variations to avoid.

But first, a few definitions: The crimes below are best categorized as 'phishing', or in some cases, targeted 'spear phishing'. They are not 'hacks'. A hack is an infiltration attempt, generally remote access or remote control.

Social engineering is a fancy name for something obvious. It's when you walk into a building wearing a technician's uniform and say "I'm here to fix..." whatever. Confidently. With a tool bag. The front desk staff (guard, office manager, whomever) glances up and says "Back left door..." and at that point, you have full access to everything. Just look like you belong there.

There are longer definitions for social engineering, but that sums it up. Make your security request look real, and it will be accepted by someone. For more background, look up any book by Kevin Mitnick, but first, look up his biography on Wikipedia. He was a famous hacker, who served 5 years in jail for breaking into corporate networks back in the mid-1990's. His book The Art of Deception is not technical; it's all about social engineering. Nowadays, he's a vice president at KnowBe4, a company that teaches computer users to recognize security issues.

Now, in email, social engineering is basically an attempt to have you respond to an email by typing a password or doing something you shouldn't. While the usual issue that you know about is opening an attachment, proper anitivirus software can deal with that. The issue is that you can get an email that is something like these REAL EMAILS:

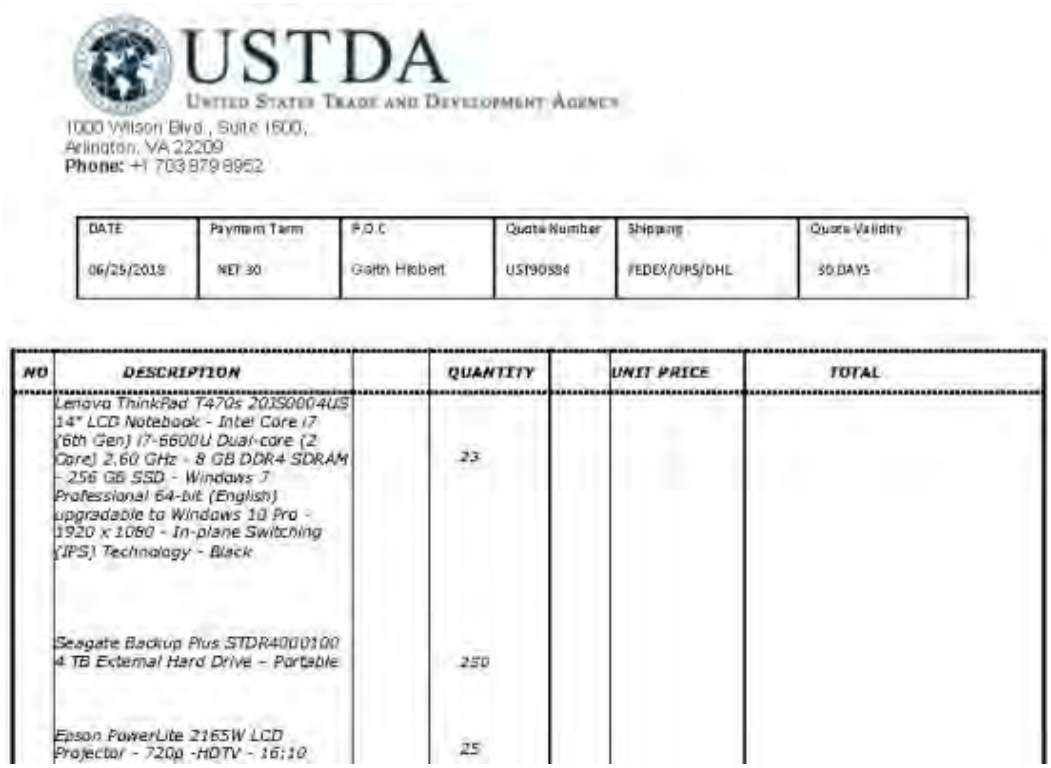
Fake Purchase Order

The U.S. Trade and Development Agency (USTDA) would like to request a quote for bidders from your company.

Attached to this RFP is the list of products requested Laptops, Projectors and other Accessories.
Best Regards.

Garth Hibbert
Chief, Office of Acquisition Management
USTDA

There's nothing dangerous about the email itself. Here's part of the attached document:



USTDA
United States Trade and Development Agency
1000 Wilson Blvd., Suite 1600,
Arlington, VA 22209
Phone: +1 703 879 8952

DATE	Payment Term	P.O.C	Quote Number	Shipping	Quote Validity
06/25/2018	NET 30	Garth Hibbert	UST90884	FEDEX/UPS/DHL	60 DAYS

NO	DESCRIPTION		QUANTITY		UNIT PRICE	TOTAL
	Lenova ThinkPad T470s 20JS0004US 14" LCD Notebook - Intel Core i7 (6th Gen) i7-6600U Dual-core (2 Core) 2.60 GHz - 8 GB DDR4 SDRAM - 256 GB SSD - Windows 7 Professional 64-bit (English) upgradable to Windows 10 Pro - 1920 x 1080 - In-plane Switching (IPS) Technology - Black		23			
	Seagate Backup Plus STDR4000100 4 TB External Hard Drive - Portable		250			
	Epson PowerLite 2165W LCD Projector - 720p -HDTV - 16:10		25			

Those items would cost around $70,000, for 23 computers, 250 external hard drives, and 25 video projectors. Big order. There's a mailing address in the email, and it's correct for that agency, and a logo, which is correct but looks like a screen capture. It's not an attempt to install malware.

I've replied to some of these. Doesn't matter what price I quote, or if I tell them to buy it from Amazon for less. They reply that they want it shipped today, net 30 terms. They either want the hardware shipped to somewhere that's not the official address of the agency, or in some cases charged to multiple credit cards with consecutive numbers, which is impossible. On that message, I looked up the credit card-issuing bank, and called their security group. They confirmed that the cards were not yet known as stolen, that the shipping addresses were wrong, and that the transactions would have been authorized, but were clearly fraudulent, and thank you for notifying us. Other banks were not so nice; there are banks that will not allow accept phone calls from merchants.

Fake Contest

FedEx.

Address : FedEx World Service Center Landmark Plaza Building,
Al Hamdan Street - Abu Dhabi - United Arab Emirates.
Tel: +971589084034
Fax: +971 4-331-0718
Email: info@fd-xae.com
Website: http://www.f-dxae.com/

We are pleased to inform you of the result of the just concluded Facebook annual Final draws powered by FACEBOOK group in cash Promotion and APPLE COMPANY to encourage all Facebook users worldwide. The co-founder of Facebook, and currently operates as its chairman and chief executive officer Mark Zuckerberg - Computer Programmer, Philanthropist - has decided to boost Users and Companies a WINDOW OF OPPORTUNITY by Lottery Program and Initial Public offer, the lottery program which is a new innovation by FACEBOOK.COM, is aimed at saying (A BIG THANK YOU) to you all our users for making FACEBOOK your number one SOCIAL NETWORK to hook up with families, friends and business partners all over the World. We are delighted to inform you that you have won a prize money of three million, and six hundred and twenty thousand US Dollars ($3,620,000USD) and Apple Mac Book Pro and the new Apple iPhone (X) 256GB mobile phone. The online draw was conducted by a random selection of EMAILS and you were picked by an advanced automated random computer search from the FACEBOOK.COM. The Prize promotion was organized by FACEBOOK.COM International Lottery Award programs held in ABU DHABI.

For your information, the FACEBOOK Company has paid the Delivery fee and Security keeping fee & Shipping charges as well as the Vat fees. You will have to pay a sum of $280.00 USD to the FedEx Delivery Department being payment for the insuring of your package. All you have to do is to insure your winning parcel with the Insurance Company, which is registered with FedEx United Arab Emirates. The reason why you are being ask to pay for the Insurance fee is because of the fact that all items & packages that is not Insured by the insurance company of United Arab Emirates are not allowed to be delivered to their delivery address. So you are to pay the FedEx Courier Service the insurance fee to enable the insurance company insured your winnings for delivery.

As soon as you effect the payment our delivery team will take your insurance fee, they will proceed to the

OK, obviously not a native speaker of English. And the email address that sent it matches a web site that is in Portugese, and sells life insurance. And the Fedex logo looks like a pasted screen capture. They're trying to collect $280 of 'shipping costs and insurance' and collect account information.

Fake Email notice

Again, this one arrived in my email. As I run the email for my own account, and I didn't send it, OK, obvious, but it should be obvious to anyone that it is not remotely possible.

Server Message

Dear [redacted]

Our record indicates that you recently made a request to deactivate email [redacted] And this request will be processed shortly.

If this request was made accidentally and you have no knowledge of it, you are advised to cancel the request now

Cancel De-activation

However, if you do not cancel this request, the your account will be de-activated shortly and all your email data will be lost permanently.

Regards.
Email Administrator

This message is auto generated from E mail security server, and replies sent to this email can not be delivered.
This email is meant for: [redacted]

Note that everything in that email is generic, except the email address. That's all the bad guys know in this case. The link goes to this screen, also 100% generic, other than the same email

address.

It's a sloppy fake, left over from some other scam; it's not even a 'cancel' message to match the email, but an 'upgrade my mailbox' message. I "logged in" with a gibberish password, and it just re-displayed the same page. I'm sure that providing a real password would have resulted in thousands of emails being sent from my account. Probably totally automated.

Fake Bank Transfers

When a social engineer knows more about you, they can do more. These would be considered "spear phishing" attacks, and the dollar amounts are far larger.

- There are scams sent to anyone known to be selling a house, claiming to be from the settlement agent, asking for bank information for the upcoming settlement bank transfer for the net proceeds of the sale. Such as transfer is fake, overseas, and as such, usually impossible to reverse.
- There are requests to transfer money from bank accounts, allegedly from the boss of a corporation, to a third party. These require more knowledge of a company, to know who would send such instructions, and who could tell the bank to setup a transfer. Always call for verification on emailed transfer orders. The numbers are large, and the transfers are not reversible.
- And finally, the IRS is a constant theme in email scams (and phone scams), and ask for information that will allow account access, or that can redirect refunds. The IRS has a list of scams, here:

https://www.irs.gov/newsroom/tax-scamsconsumer-alerts

Always look at the sending email address; that's the biggest confirmation of fakes, IRS-themed or otherwise. The IRS does not send email from a .com address. Actually, they don't send email at all for important matters; account-specific IRS messages use paper mail. Not email, and never robocalls.

The Federal Trade Commission is also a great source for learning how to recognize email and tech scams. Here is their page on scams against small business; the PDF at the top of the page is a good summary for your co-workers:

https://www.ftc.gov/tips-advice/business-center/guidance/scams-your-small-business-guide-

business

Overall, these email scams will sometimes look fake, with mis-spelled words, clumsy English, nouns capitalized that normally are lower-case, over-the-top claims of way too much money, and an implied sense of urgency and scary warnings that you will lose something.

Be suspicious. Always look at links before you click by floating the mouse over the link–it shows up at the bottom of your screen. And if it sounds too good, it's probably phishy.

Thunderstorm Season

It's that time of year.

- Check that your technology, especially anything that connects to your computer with a cable, is on a modern surge suppressor.
- Check your computer backups. Lightning strikes mostly destroy power supplies and network cards, but a direct strike at the power pole will fry everything. Backups are the best protection against data loss.
- If you're going on vacation, consider unplugging your technology while you're gone if it's not working for you. That's not "turn off" but un-plug. Most electronics that are "off" are really "on, not doin' much, just keeping the clock running, waiting for a quick startup by keeping memory turned on." In other words, they're connected to power lines.
- Again, unplug backup drives during vacations. Lock them up elsewhere.

Contact

Address all editorial and unsubscr be requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158

Phone (410) 871-2877