Scams!

PAULETTE WOOLF AND MELISSA DUBINSKY

NETANYA AACI

12 DECEMBER 2021

2

Phishing

Not to be confused with Fishing or Pishing

Phishing

- **Phishing** is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a human victim into revealing sensitive information to the attacker

Three kinds of problems

- You innocently answer innocent questions – how can that be a problem? It's just fun!
- You respond to a call or request to provide real information (one time codes, passwords, "last four digits of credit card", etc.) – but it is the scammer calling
- You are pressured emotionally to responding

Ways scammers get your personal information

- Phone
- Text messages (SMS)
- WhatsApp broadcast messages
- Email
- Facebook

Camouflage

- Caller ID shows a real name "IRS" but it is a scammer
- Email address seems real
- Logo on a letter seems real
- Caller knows a lot of your personal information, including about your family – but still a scam
- Appeals to your emotions – your grandchild is in trouble and you are the only one who can wire the money; you will go to jail if you don't settle this bill immediately

How it works

- Small pieces of information get collected and aggregated by "data miners"
- Innocent questions are mixed with important questions
- When you answer, all your friends are accessed as well
- "Liking" or "Unsubscribe" or "Click to open the link" proves that you are real with a real email
- Pretty soon "they" know everything they need to know about you to steal your identity, access your bank accounts, etc.

Telephone scams

- Telephone scammers try to steal your money or personal information.
- Scams may come through phone calls from real people, robocalls, or text messages.
- Callers often make false promises, such as opportunities to buy products, invest your money, or receive free product trials. They may also offer you money through free grants and lotteries. Some scammers may call with threats of jail or lawsuits if you don't pay them.
- Be cautious of caller ID. Scammers can change the phone number that shows up on your caller ID screen. This is called "spoofing."

Hang up on suspicious phone calls.

Avoiding telephone scams: Don't....

- Don't give in to pressure to take immediate action.
- Don't say anything if a caller starts the call asking, "Can you hear me?" This is a common tactic for scammers to record you saying **"yes."** Scammers record your "yes" response and use it as proof that you agreed to a purchase or credit card charge.
- Don't provide your credit card number, bank account information, or other personal information to a caller.
- Don't send money if a caller tells you to wire money or pay with a prepaid debit card.

10

Social Security or similar scams

If you receive a call, SMS or email that:

- Threatens to suspend your **Social Security number**, even if they have part or all of your Social Security number
- Warns of **arrest of legal action**
- Demands or requests **immediate payment**
- Requires payment by **gift card, prepaid debit card, internet currency, or by mailing cash**
- Pressures you for **personal information**
- Requests **secrecy**
- Threatens to **seize your bank account**
- Promises to increase your Social Security benefit
- Tries to gain your trust by providing **fake "documentation," false "evidence," or the name of a real government official**

...it is a SCAM!

Protect yourself and others from scams

- **Try to stay calm.** Do not provide anyone with money or personal information when you feel pressured, threatened, or scared.
- **Hang up or ignore it.** If you receive a suspicious call, text, or email, hang up or do not respond. Government employees will not threaten you, demand immediate payment, or try to gain your trust by sending you pictures or documents.
- **Report scams.**
- **Get up-to-date information on scams.**
- **Spread the word. S**hare your experience and warn others.

Giving up information

- The call came from PayPal's fraud prevention system. Someone had tried to use my PayPal account to spend $58.82, according to the automated voice on the line. PayPal needed to verify my identity to block the transfer.
- "In order to secure your account, please enter the code we have sent your mobile device now," the voice said. PayPal sometimes texts users a code in order to protect their account. After entering a string of six digits, the voice said, "Thank you, your account has been secured and this request has been blocked."
- "Don't worry if any payment has been charged to your account: we will refund it within 24 to 48 hours. Your reference ID is 1549926. You may now hang up," the voice said.

- https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo?fbclid=IwAR0BX3CtJHCenxh2AOOcED4eYXPtQMEU_KHPymomjwkBSEUah0lIq6Jlc3g

Harmless questions

- One of these has to go" with a list of four types of candy bars
- "how old would you be if the digits in your age were reversed."
- "your birth month determines which celebrity you marry, are you happy?" with a bunch of pictures of famous people laid out in a calendar grid.

Games to get you to list personal information

- Common security questions: maiden names, grandparents' names, where you vacationed as a kid, what was your first car, what was your first pet's name, what was the name of your elementary school.

Result: Fraudsters can cash into your accounts

- "They" can either get into your bank account, sell your information to someone else who wants to get into your bank account, or remotely lock your accounts or take over your whole computer or phone and force you to pay a ransom to get access back.
- "They" can impersonate you and steal your tax refund. They can commit social security fraud, pretending to be you, and disappear with the check while you are left to prove it wasn't you.

To break into an account

- Hacker needs a victim's username or email address and password.
- Obtainable from a previous data breach which contains credentials many people reuse across the internet.
- Or they could buy a set of "bank logs"—login details—from a spammer.
- Bank employees won't call, text or email consumers asking for this info, but crooks will.

- https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo?fbclid=IwAR0BX3CtJHCenxh2AOOcED4eYXPtQMEU_KHPymomjwkBSEUah0lIq6Jlc3g

Appliance insurance scam techniques (Pressure Sales)

- The installer tells you he cannot leave unless you pay for appliance insurance
- The installer tells you that you already signed up for it (committed to get it) but you must pay him
- Someone calls you to “renew” your annual insurance policy (even if you never had one)

NETFLIX Scam

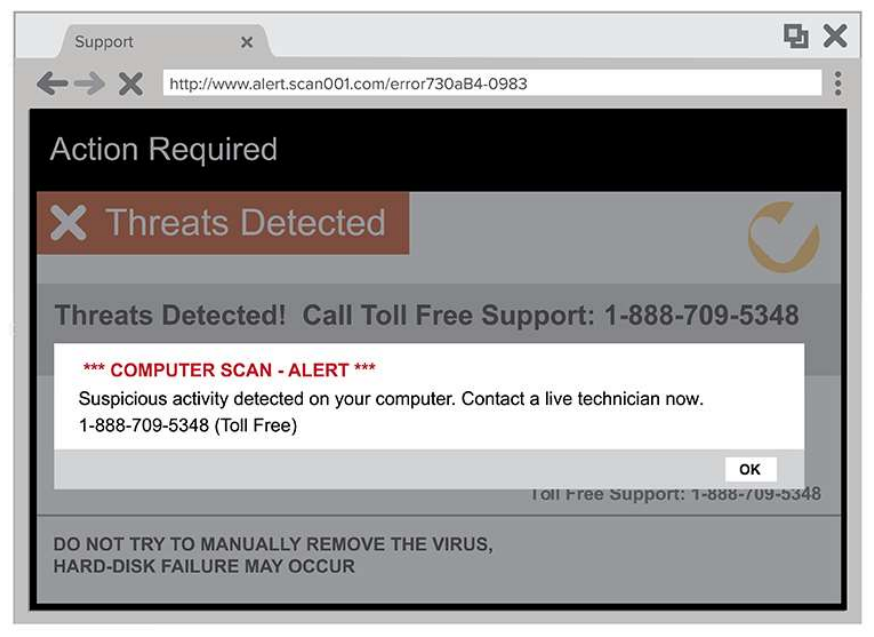
How do you know it's a scam?

- The email looks like it's from a company you may know and trust: Netflix. It even uses a Netflix logo and header.
- The email says your account is on hold because of a billing problem.
- The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email invites you to click on a link to update your payment details.

Tech support scams

- Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services you don't need, to fix a problem that doesn’t exist.
- Tech support scammers may call and pretend to be a computer technician from a well-known company. They say they’ve found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn’t exist.
- ***If you get a phone call you didn’t expect from someone who says there’s a problem with your computer, hang up.***

Computer scam – Pop-up window



Pop-up warnings

- Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.
- ***If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.***

Online ads and listings in search results pages

- Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online. The scammers are hoping you'll call the phone number to get help.
- ***If you're looking for tech support, go to a company you know and trust.***

Avoid Tech Support Refund Scams

- If someone calls to offer you a refund for tech support services you paid for, it's likely a fake refund scam.

How does the scam work?

- The caller will ask if you were happy with the services you got. If you say, "No," they'll offer you a refund. In another variation, the caller says the company is giving out refunds because it's going out of business. No matter their story, they're not giving refunds. They're trying to steal more of your money.
- Don't give them your bank account, credit card or other payment information.

What To Do if You Think There's a Problem With Your Computer

- If you think there may be a problem with your computer, update your computer's security software and run a scan.
- If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

What To Do if You Were Scammed

- If you paid a tech support scammer with a credit or debit card, you may be able to stop the transaction. Contact your credit card company or bank right away. Tell them what happened and ask if they can reverse the charges.
- If you paid a tech support scammer with a gift card, contact the company that issued the card right away. Tell them you paid a scammer with the gift card and ask if they can refund your money.
- If you gave a scammer remote access to your computer, update your computer's security software. Then run a scan and delete anything it identifies as a problem.
- If you gave your user name and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.

Banking scams

- **Overpayment scams -** Someone sends you a check, instructs you to deposit it in your bank account, and wire part of the money back to them. But the check was fake, so you'll have to pay your bank the amount of the check, plus you'll lose any money you wired.
- **Unsolicited check fraud** - A scammer sends you a check for no reason. If you cash it, you may be authorizing the purchase of items or signing up for a loan you didn't ask for.
- **Automatic withdrawals** - A scam company sets up automatic withdrawals from your bank account to qualify for a free trial or to collect a prize.
- **Phishing** - You receive an email message that asks you to verify your bank account or debit card number.

Investment scams

- Investment scams – if it sounds too good to be true – it probably is. Friends who are innocently involved in a scam may try to pull you in….
- Don’t give in to pressure to invest immediately.
- Don’t be influenced by promises that seem too good to be true. These promises may include “guaranteed earnings” or “risk-free” investments.
- Don’t invest just because the investment professional seems nice, trustworthy, or has professional titles.
- Don’t invest based on claims that other people, "just like you", have invested.
- Don’t feel obligated to invest, even if the professional gave you a gift, lunch, or reduced their fees.

Other kinds of scams

- Post office scam – send money to collect a package
- Lottery and sweepstakes scams – i.e., you've won a prize but must pay money to collect it
- Charity scams – fake charities to take advantage of a disaster somewhere
- Pyramid scams – "multi-level marketing" (mathematically guaranteed to fail!)
- Ponzi scams – investment based pyramid scam (also mathematically guaranteed to fail!)
- Ticket scams – fake tickets, or paid for and never received
- Auto-renewals – appliance warrantees, charitable annual donations, etc.

Four Steps To Protect Yourself From Phishing (1)

- **1. Protect your computer by using security software**. Set the software to update automatically so it can deal with any new security threats.
- **2. Protect your mobile phone by setting software to update automatically.** These updates could give you critical protection against security threats.

Four Steps To Protect Yourself From Phishing (2)

- **3. Protect your accounts by using multi-factor authentication.** Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication, such as:
- Something you have — like a passcode you get via an authentication app or a security key.
- Something you are — like a scan of your fingerprint, your retina, or your face.
- Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.
- **4. Protect your data by backing it up.** Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What To Do if You Suspect a Phishing Attack

- If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I have an account with the company or know the person that contacted me?**
- **If the answer is "No,"** it could be a phishing scam. Go back and review the tips in How to recognize phishing and look for signs of a phishing scam. If you see them, report the message and then delete it.
- **If the answer is "Yes,"** contact the company using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.

What To Do if You Responded to a Phishing Email

- If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov (in the US). There you'll see the specific steps to take based on the information that you lost.
- If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan.

Take-home Messages

- There are plenty of "bad guys" trying to get data and they are more clever than you.
- When it doubt, and even if you have no doubt, say NO. You can always follow up separately later.
- Never say YES on a phone call from someone you don't know, not even "Is your name ***" – they can splice the YES to "prove" you said YES to giving them your money

More take-home messages

- If it sounds too good to be true, you can be sure it is
- No financial institution makes you give information urgently. The more urgent the request, the more likely it is to be a scam
- NEVER respond to innocent questions ("how many of these have you done as a child", "click your favorite movie star", "what candy bar can you live without")
- Don't click "LIKE" unless you know the person you are responding to (and never to anything with thousands of respondents)
- Never give personal information to someone who contacts you by any means (phone, SMS, Facebook, email). Tell them to send an email. Don't let them give you a phone number to check up on them. Find the phone number yourself

Thank you!