Security Awareness Remastered

QUICK REFERENCE

Common Scams

1. Avoiding Gift Cards Scams
2. Avoiding QR Code Scams
3. Avoiding Fake Job Scams
4. Avoiding Tech Support Scams
5. Avoiding Fake Check Scams

Protect Yourself

6. Never Share Verification Codes!
7. Prevents Apps from Stealing Your Data
8. Lie on Your Security Questions
9. Two Factor Authentication
10. Is Privacy a Myth?

Protect Your Company

11. Staying Safe on Public WiFi
12. USB Safety
13. Choosing Strong Passwords
14. Shadow IT
15. Social Media Security
16. Preventing Mobile Security Threats
17. Phishing Examples
18. Detecting a Phishing Attack
19. What is BEC?
20. Avoiding BEC Attack
21. What is Smishing?
22. What is Vishing?
23. What is Ransomware?
24. Avoiding Ransomware

1 Common Scams

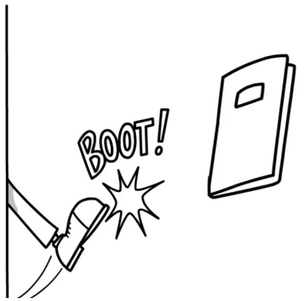
Avoiding Gift Card Scams

- Always call or verify the sender in person for any request for you to purchase gift cards.
- If it sounds like a strange request, it probably is.
- Don't open gift cards from people you don't know.

2

Avoiding QR Code Scams

- Many restaurants started putting QR Codes on tables instead of menus during the pandemic. Criminals are replacing them with their own!
- Try to avoid scanning QR Codes. Instead, ask for the official URL.
- QR Codes can be replaced in more than just restaurants.
- If you scan a QR Code, make sure you are on the right website and if you are asked to do anything, don't.



3

Avoiding Fake Job Scams

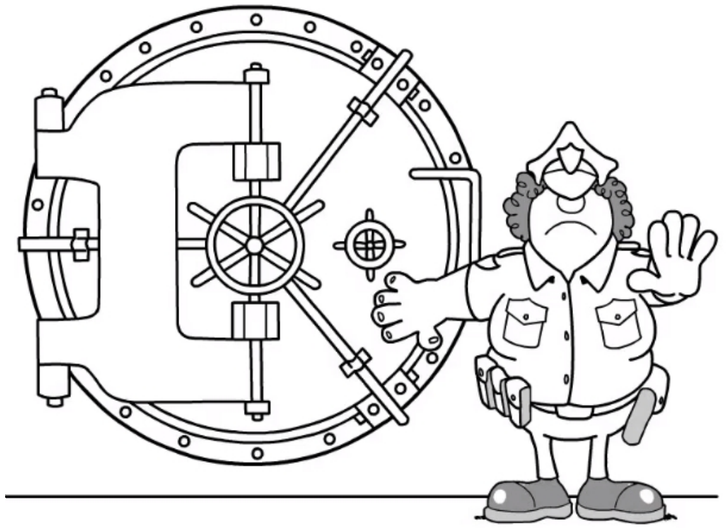
- Criminals take advantage of job hunters by using their personal information to steal their identity or by sending them infected documents and links.
- Companies offering you advances are suspect.
- Interviews are not normally conducted over text message. Request a video chat if an in person interview is not available.
- Don't share personal or banking information early in the process.
- If it's too good to be true, it probably is.

Avoiding Tech Support Scams

- Scammers purchase domain names that look similar to actual websites. They clone the website to make it look legit.
- Call and verify a tech support business before you click. Verify the phone number by checking it on the actual website.
- Phone numbers can also be fake or "off" by one number to get you to misdial. If the call doesn't feel right, verify the number and call again.
- A scammer may fake a business listing on Google Maps, so verify the phone number with the official website.

Avoiding Fake Check Scams

- Criminals can pretend to be someone that owes you money. They send you a check. You deposit it. They claim they overpaid. You pay them back the difference. Their check doesn't clear the bank and you are out of money.
- Accept only cash in person if you are selling something.
- If you receive a check, verify the person or company that gave it to you. Call the official company to verify its authenticity.
- If something doesn't feel right, don't deposit the check.

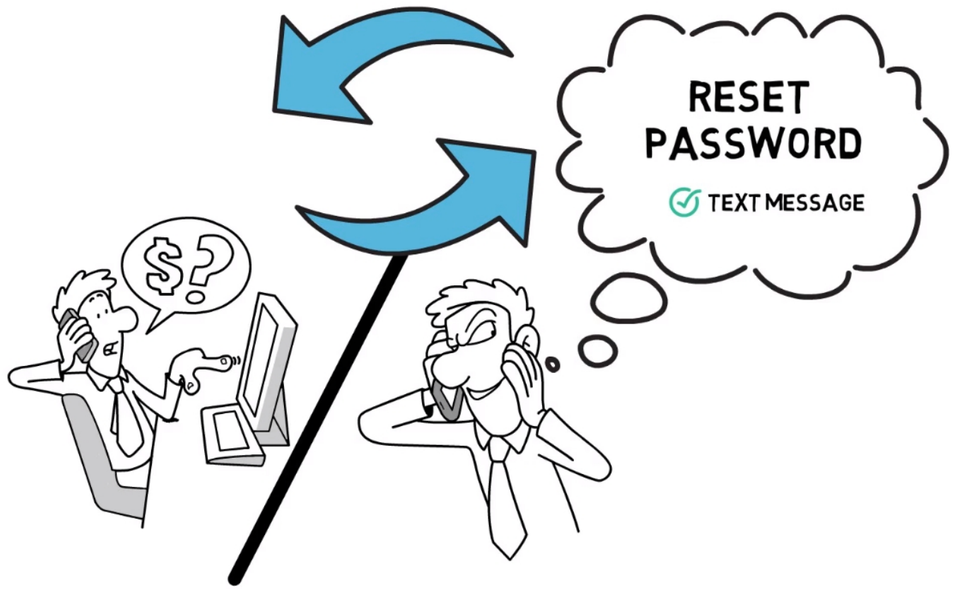


6 Protect Yourself

Never Share Verification Codes

- Scammers call pretending to be from a credit card fraud division or some other company and ask you to share your verification code with them. They've actually just reset your password instead and can now access your account.

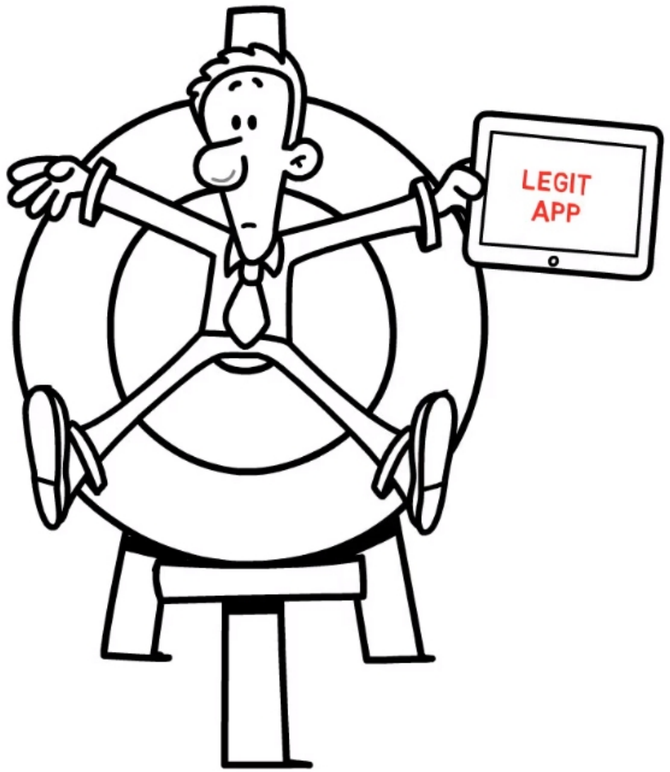
- Never share verification codes no matter what.



7

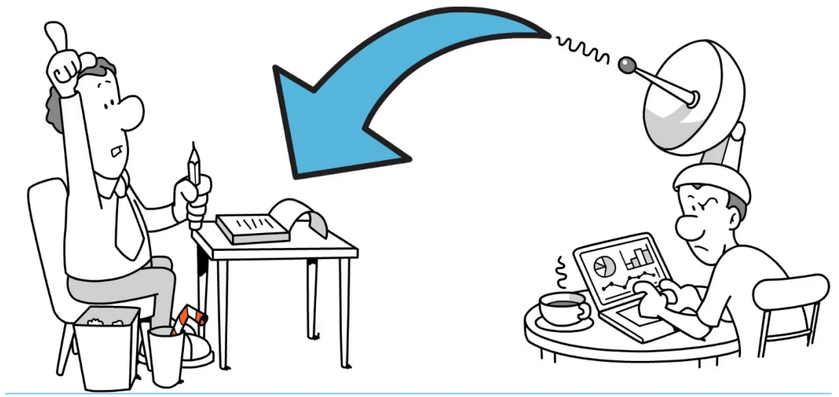
Prevent Apps from Stealing Your Data

- Criminals may create legit looking apps that may steal people's personal information from their devices.
- Only download apps from trusted places like Google Play or the Apple Store.
- Delete apps you no longer use.
- Don't allow apps lifetime access to your photos or contact list unless it is absolutely necessary. Use the settings to control access.



Lie on Your Security Questions

- If scammers can find out answers to common questions about you, they can use the answers to access your accounts by answering security questions.
- They can find these answers on background check sites that scan the web for your information or on social media sites.
- Always lie on security questions!
- Nothing online is 100% private! Be careful what you share.

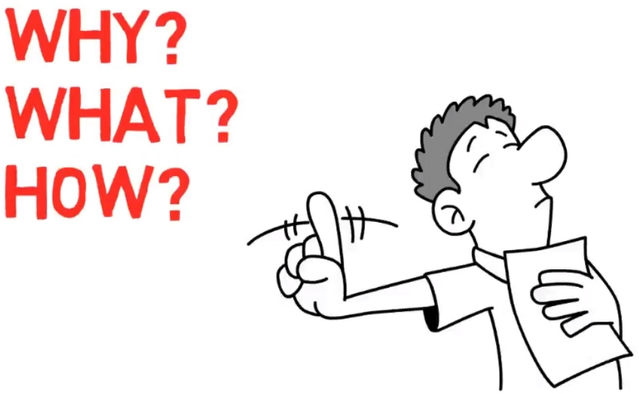


Multi-Factor Authentication

- If you use the same password for multiple websites and your password is stolen, all of those accounts are now at risk.
- Using Multi-Factor Authentication verifies that YOU are YOU. This is done by sending a code by text message or through an authentication app.
- Using Multi-Factor Authentication prevents a scammer from accessing your account, even if they know your password.
- Multi-Factor Authentication is usually turned off on most sites by default. Be sure to turn it on.

Is Privacy a Myth?

- Nothing online is 100% private.
- Some things should NEVER go online like private photos.
- Some things should be verified: Like someone asking for your social security number. Ask why they need it, what they need it for, and how they will protect it.
- Some things should require a strong and unique password: Things that we care about but it won't be the end of the world if they are exposed... like a Google Doc that contains a list of your family members.
- Some things are OKAY to share: These are things you want everyone to know, like how cute your dog is.



11 Protect Your Company

Staying Safe on Public WiFi

- Connect to legitimate WiFi only.
- Avoid websites that expose personal, financial, or organization information.
- Use a firewall and Virtual Private Network (VPN.

USB Safety

- Delete contents when not needed.
- Protect with a password and encrypt the data.
- Change passwords stored on a USB if it becomes lost or stolen.

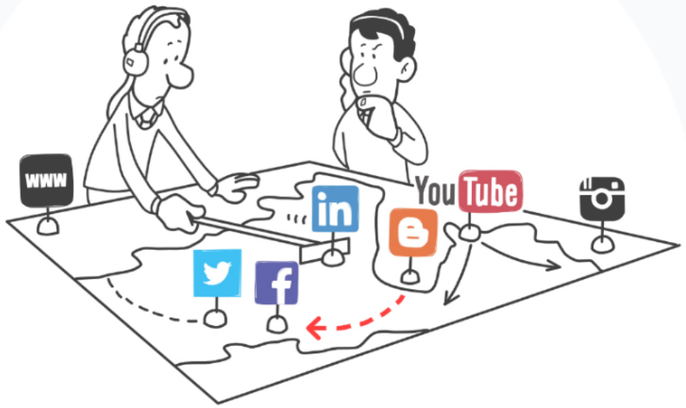
Creating a Strong Password

- Step 1 - Think about at least 3 things you like. (vacations, books, music)
- Step 2 - Combine the 3 words to form the initial password. (vacationsbooksmusic)
- Step 3 - Add a special character in between these words. (vacations$books$music)
- Step 4 - Add a number you can remember to the end of the password. (vacations$books$music1402)
- Step 5 - To make it unique for different websites, append the website name to the end of the password. (vacations $books$musicFB) - FB for Facebook

Shadow IT - The hidden Dangers

- Avoid using shadow IT for critical organization applications.
- Limit Shadow IT to personal productivity tools, time tracking, and blogging.
- Make a case to your IT department if you want another application, system, or program.

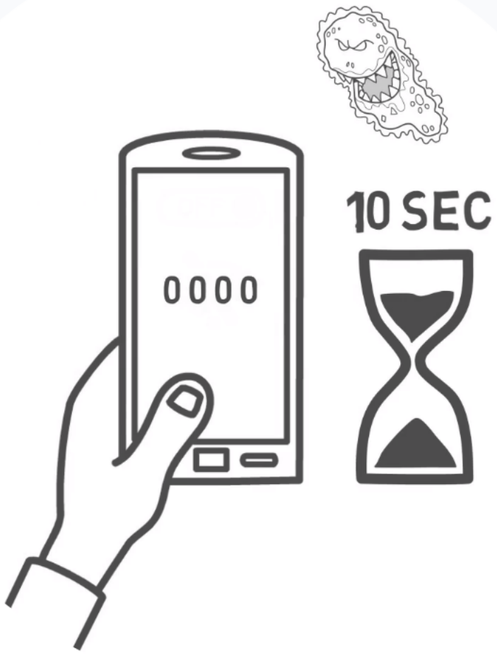
Social Media Security



- Verify posted links, downloads, or email attachments before clicking.
- Avoid naming or referencing customers, partners, or suppliers.
- Never disclose personal or confidential organization information.
- Use different passwords for social media than used to access organization accounts.
- Only speak for yourself and not on behalf of another person or organization.

Preventing Mobile Security Threats

- Disable Bluetooth and WiFi when not in use.
- Change the device default password ASAP.
- Download apps only from the Apple Store or Google Play Store.
- Never "jailbreak" a device.
- Update mobile devices often.



Common Phishing Examples

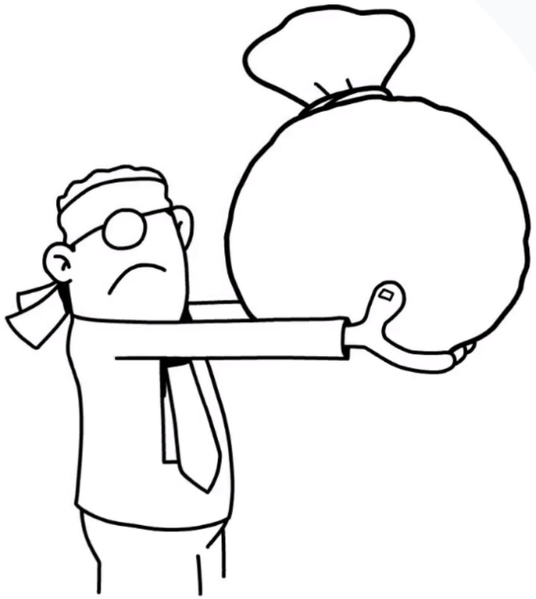
- A fake Dropbox email with a link to a virus
- A message from your IT department asking you to reset your password
- A fake invoice on behalf of a vendor with fraudulent wire instructions
- A phishing email from HR requesting your W-2
- Fedex/UPS alerting you about an issue with your package

How to Detect Phishing

- Hover over the link in the email and verify it is pointing to the official website.
- Verify that the sender’s email is correct and does not include spelling mistakes.
- If the browser address bar warns you that “this website is not secure”, close it.
- If you click on a link, make sure the address bar displays the official website.
- If you need to login to a website, manually type the address instead of clicking a link.
- Don't open attachments you’re not expecting.

What is BEC

- When a hacker impersonates an executive (e.g. CEO, County Executive\Administrator, City Manager, etc.) or vendor in an attempt to gain access to sensitive information or funds
- Typically comes in an email phishing attack with the sender's email address spoofed – from your ceo@organization.com
- Attack is often an urgent email to the financial department with fraudulent wire instructions



Avoiding BEC Attack

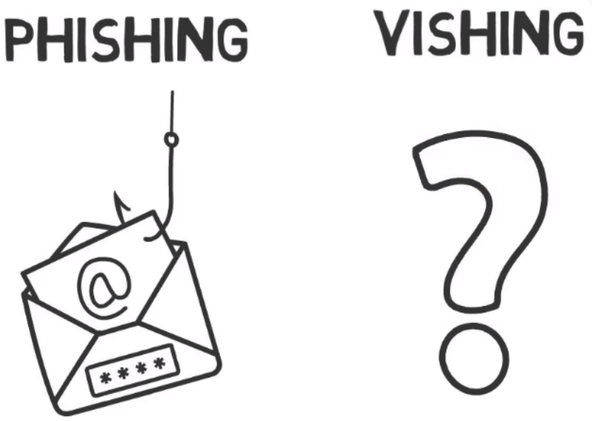
- BEC Identification Tips
  - Email typically possesses a sense of urgency
  - Style is unusual and short, often with spelling and grammar mistakes
  - Email address is spoofed or has a slight spelling mistake
- Never hit reply. Instead, manually type the email of the sender.
- Call the sender over the phone and verify the request.
- Verify that the bank account matches the one in your accounting system.
- Always follow organizational protocol and procedures.

What is Smishing

- Smishing is a mobile scam that works like phishing, but via text.
- Common examples:
  - Past due payments from a service provider
  - Unauthorized access warnings from your bank
  - You won a prize.
- Always call the official number of the organization in question. If they can't verify the content of the message, ignore it.

What is Vishing

- Vishing is when an attacker poses as someone you trust over the phone.
- Common examples:
  - Your bank calling about suspicious activity on your account
  - The IRS calling about overdue or unpaid taxes
  - An "all-expense" paid vacation
  - Tech support calling to remotely access your PC
- Never give up passwords or other sensitive information to anyone over the phone.



What is Ransomware

- Ransomware is malicious software that takes control over your computer and denies you access to your own data
- Once your PC is infected, the hacker demands payment to restore control
- Government agencies and medical facilities are common targets due to their dependence on data to operate
- Phishing emails are one of the most common methods hackers use to infect a PC with Ransomware

Avoiding Ransomware

- If an unsolicited email, phone call, text, or instant message is received, do not give out any personal information, open attachments, or click any links.
- If you are unsure about the authenticity of the message, then consult with IT.
- Use a Virtual Private Network (VPN) when outside the office .
- Keep computers and devices patched, up to date, and make sure anti-virus software is installed.
- Don't install software or give administrative privileges to any program.
- Backup your files frequently.