Info Security MPAFUG 2025 Edition

Presented by: Bill Heck , January 8, 2025

Who Am I?

- Bill Heck
  - Team Manager, Optiv Security
  - Specialty in Application Security
  - IT / Info Security for over 30 years
  - Part-time Musician

Scams - Know how to identify one

SMS / Text Scams

Passwords and Password Databases

Agenda Multi-Factor Authentication

AI and Voice Cloning

Delivery Scams

New Year's Resolutions

Trivia - Learn to Identify Scams

Scams

Is it a Scam?

1. Scammers PRETEND to be from

Scammers often pretend to be contacting

organization you know. or on behalf of the government. They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.

They use technology to change the phone

number that appears on your caller ID. So

the name and number you see might not be

real.

Is it a Scam?

2. Scammers say there's a PROBLEM

They might say you're in trouble with the

government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer.

Some scammers say there's a problem with one of your accounts and that you need to verify some information.

Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

Is it a Scam?

3. Scammers PRESSURE you to act immediately. Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story.

They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

Is it a Scam?

4. Scammers tell you to PAY in a specific way. They often insist that you pay by sending money through a money transfer company or by putting money on a gift card

and then giving them the number on the back.

Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money.

SMS (Text) Scams

More Texts I've Received…

Passwords and Password Databases

Weak passwords

Still being used in 2024

Password Security

Use a different password for each of your important accounts, like your email and online banking.

Reusing passwords for important accounts is risky. If someone gets your password for one account, they could access your email, address, and even your money.

Long passwords are stronger, so make your password at least 12 characters long. These tips can help you create longer passwords that are easier to remember.

Try to use:

- A lyric from a song or poem
- A meaningful quote from a movie or speech
- A passage from a book
- A series of words that are meaningful to you
- An abbreviation: Make a password from the first letter of each word in a sentence
- Using a random string of characters is significantly more secure use a Password Manager.

Password Managers

- Store your passwords
- Generate strong passwords
- Remind you to change your passwords

Examples

- KeePass (KeePassX)
- Keeper
- Bitwarden
- NordPass
- 1Password
- RoboForm
- Passwords (MacOS)

Password Manager Demo

Multi-Factor Authentication

Multi-factor authentication is the process of identifying users by validating two or more "factors," or characteristics that are unique to that user.

Three different characteristics are often used as factors in the authentication process:

- something you know
- something you have

● something you are

If Multi-Factor Authentication is available, USE IT!

Artificial Intelligence - AI

● The big unknown

● Advancement in Voice Cloning

○ Grandparent /

Grandchild scam

○ “Yes” scam

● Scams using voice Cloning

(video)

Artificial Intelligence - AI Voice Cloning

Delivery Scams

How to avoid delivery scams

● Keep track of your deliveries. Scammers hope you'll just assume they are talking about a package you ordered recently, without double-checking. It will be much harder for them to fool you if you know what packages you are expecting, from what companies, and when.

● Know delivery company policies. Delivery companies will never contact you with unsolicited calls or texts. Depending on how you signed up for notifications, messages usually are posted within a secure online portal. Be leery of unsolicited messages, especially if you never signed up for text alerts.

● Never give sensitive personal information to strangers. If an unsolicited caller asks you for personal information, even if they claim to represent a company you trust, hang up and call the company using the official customer service number. Calling the company yourself is the best way to determine if the inquiry is legitimate or a scam.

New Year’s Resolutions

2025 Security New Year's Resolutions

● I will be cautious with email. Be wary of unsolicited emails from a person or a company. Remember, scammers can make emails look like they are from a legitimate business, government agency, or reputable organization (even BBB!). Never click on links or open attachments in unsolicited emails.

● I will never send money to strangers. If you haven't met a person face-to-face, don't send them money. This is especially true if the person asks you to transfer funds using a pre-paid debit card or CashApp. Money sent to strangers in this way is untraceable, and once it is sent, there's no getting it back. Scammers will try to trick you into panicking – so before making a move, think the situation through.

Don’t fall for it!

● I will do research before making online payments and purchases.

Research the retailer before entering payment information when shopping online, or if asked to pay online, research the

retailer before entering payment information.

Ask: Is this a person or business I know and trust? Do they have a working customer service number?

Where is the company physically located? Would I be making payments through a secure server (https://....com)?

Have I checked to see if others have complained?

● I will use my best judgment when sharing my personal information.

Sharing sensitive personal information with scammers opens the door to identity theft. Never share financial information, birthdate, address, Social Security/Social Insurance number, or Medicare number with an unsolicited caller.

2025 Security New Year's Resolutions

● I will create strong, unique passwords for each account. Using strong, varied passwords across accounts makes it harder for fraudsters to access multiple accounts if one is compromised.

● I will enable two-factor authentication. Adding this layer of security to accounts, especially those involving finances or personal data, greatly reduces the risk of unauthorized access.

● I will be social media smart. Use privacy settings on social media and only connect with people you know. Be careful about including personal information in your profile, and never reveal your address and other sensitive information – even in a "fun" quiz. Scammers may use this information to make themselves pass as friends or relatives and earn your trust. Also, be careful when buying products you see on social media. BBB Scam Tracker has received thousands of complaints about misleading Facebook and Instagram ads.

● I will regularly check my financial statements. Committing to review bank and credit card statements can help catch unauthorized transactions early.

● I will educate myself about the latest scams. Staying informed on emerging scams helps you recognize and avoid new fraud tactics.

TRIVIA

Part 1 - Impersonation Scams

1. You receive an unsolicited text from a website you use saying that your password has been compromised. They provide a link for you to change it. You should:

A. Delete the text

B. Reply to the text to confirm that you really need to change your password

C. Follow the link and change your password

5. A pop-up on your computer tells you there is a major issue. Tech support people from a well-known technology company reach out and offer to help you, but they require immediate payment. You should:

A. Give them access to your computer so they can fix your computer as soon as possible.

B. Pay them so they can help you regain access to your computer.

C. Hang up immediately and reach out to somebody else to check your computer and determine if malware or spyware has been uploaded.

1. When paying online, which payment method offers the best protection?

A. Debit Card

B. Payment apps (such as Zelle, Venmo, or PayPal)

C. Credit card

D. Gift card

E. Wire transfer

2. If a website shows the padlock symbol in the address bar, I am safe to shop.

A. True

B. False

3. You'd like to purchase from a website you've never visited before. To protect yourself from a scam, you should do all the following except:

A. Research the age of the domain.

B. Confirm there's a padlock in the address bar to ensure my shared information is secure.

C. Research a third-party website to see if the URL has been reported as a fake website (BBB.org, BBB Scam Tracker, or another website)

D. All of the above

1. Two-factor authorization can help protect you against phishing attacks. True or false?

A. True

B. False

2. If you receive an email from the government stating that you owe money and must pay immediately, or you'll be fined. You should:

A. Click the link to make sure it is real.

B. Delete it immediately

C. Pay it immediately to avoid fines

3. Which one of these statements is correct?

A. Clicking on an unknown link is okay if you have a spam blocker

B. You can trust an email really comes from a client if it uses the client's logo and contains at least one fact about the client that you know to be true.

C. If you get a message from a colleague who needs your network password, you should never give it out unless the colleague says it's an emergency.

D. If you get an email from a family member asking you to provide personal information right away, you should contact the family member directly to see if the email came from them.

4. You get a text message from your bank informing you that your account has been compromised. It asks you to click on a link to reset your security information. You should:

A. Reply to the text to get more details about how to renew your password.

B. Pick up the phone and call the bank, using the number on your debit card or statement.

C. Click on the link to see if it is real.

1. Which of the following are “red flags” that you are experiencing an investment scam?

A. They pressure you to invest immediately or risk missing out (limited time offer).

B. They promise a guaranteed return on investment.

C. They claim to be from a reputable firm.

D. They tell you everyone’s making money. Don’t miss out.

E. All of the above.

Scams - Know how to identify one

SMS / Text Scams

Passwords and Password Databases

Summary

Multi-Factor Authentication

AI and Voice Cloning

Delivery Scams

New Year’s Resolutions

Trivia - Learn to Identify Scams

Thank You!

Bill Heck

bill.heck71@gmail.com