SCAM ALERT

5 dangerous phone scams that are spreading now

1. DHS OIG HOTLINE SCAM

The most recent scam hitting the phone lines deals with the U.S. government. The Department of Homeland Security (DHS) Office of Inspector General (OIG) just issued a fraud alert to warn citizens that the DHS OIG Hotline phone number is being used as part of a telephone spoofing scam. People from all across the country are being targeted.

The scammer pretends to be an employee with U.S. Immigration and alters the caller ID system to make it appear as if the call is coming from the DHS OIG Hotline number (1-800-323-8603). The fraudster demands that the victim verifies personal information through numerous tactics, including claiming they are victims of identity theft.

One important thing to remember is that DHS OIG *NEVER* uses its Hotline number to make outgoing calls. It's only used to receive information from the public, so you should not answer calls purporting to be from 1-800-323-8603.

If you receive a call claiming to be from the DHS OIG Hotline, do *NOT* provide personal information. The scammers are trying to get victims to reveal data like their Social Security number, credit or debit card info, date of birth, drivers license number and bank account information. They will use the data to drain your accounts and/or steal your identity.

DHS wants everyone to know that the DHS OIG Hotline continues to be safe to use to report fraud, waste, abuse or mismanagement within DHS components or programs.

If you believe that you may have already fallen victim to this phone spoofing scam you should call the Hotline or file a complaint online via the DHS OIG website. You can also contact the Federal Trade Commission to file a complaint and/or report identity theft.

2. FBI SPOOFING SCAM

There is another telephone spoofing scam similar to the DHS OIG Hotline scam but with a twist. This one purports to be a call from the FBI.

Fraudsters claiming to be FBI agents are calling people at random and telling them they are being investigated for certain federal violations. The victim is told that if they don't pay a fee immediately they will be arrested.

The call seems legitimate because the scammer spoofs the local FBI field office phone number and it displays that way on caller ID.

Warning, this is a scam!

The FBI does not call or email private citizens to demand money or threat arrests. If you are contacted by someone claiming to be with the FBI, verify the information with the Bureau. Click here to see a list of all FBI field offices in the U.S. and their contact information.

If you believe you are a victim of a phone or online scam, click here to file an online complaint with the FBI's Internet Crime Complaint Center.

3. "CAN YOU HEAR ME" PHONE SCAM

There was recently a Consumer Alert warning Americans about 'can you hear me' scams. We actually warned you about these scams making the rounds a few months ago. Now, the Federal Communications Commission (FCC) said the problem is getting worse.

The FCC is asking consumers to be careful answering calls from unknown phone numbers. Scammers are calling victims hoping to get them to say the word "yes" during the conversation that's being recorded. The fraudster will later use the recording of the victim saying yes to authorize unwanted charges on the victim's utility or credit card account.

The scam works like this: a consumer answers a call from someone impersonating a representative from organizations that provide a service that the victim is most likely familiar with. The criminal could say they're with a utility company, a mortgage lender or a credit card company to name a few.

The scammer will ask "Can you hear me?" The caller records the victim saying yes, which they later use as a voice signature. This voice signature can be used to authorize fraudulent charges via telephone.

What you need to do

The FCC is telling consumers who receive a call like this to immediately hang up the phone. If you think that you have already received a call like this, you need to check your bank and credit card statements as well as your telephone statement to see if there are any unauthorized charges.

If you find unauthorized charges, it's likely that you are a victim of what's known as "cramming." Report these charges as unauthorized ASAP.

You should also report the incident to the Better Business Bureau's Scam Tracker and to the FCC Consumer Help Center.

The FCC gave these tips to help ward off unwanted calls and scams:

- Don't answer calls from unknown numbers - This is the most obvious and simplest precaution. Let unknown calls go to voicemail.
- If you answer and the caller (often a recording) asks you to hit a button to stop receiving calls, just hang up. Scammers often use these tricks to identify and target live respondents.
- If you receive a scam call, write down the number and file a complaint with the FCC so it can help identify and take appropriate action to help consumers targeted by illegal callers.
- Ask your phone service provider if it offers a robocall blocking service. If not, encourage your provider to offer one. You can also visit the FCC's website for information and resources on available robocall blocking tools to help reduce unwanted calls.
- Consider registering all of your phone numbers on the National Do Not Call Registry.

4. WHY YOU SHOULD BE WORRIED ABOUT SMISHING

There is a new type of scam that you definitely need to be worried about. It's called "smishing," short for SMS phishing.

This new texting scam looks so legitimate, anyone could fall victim to it. Scammers are spoofing banks' phone numbers and sending text messages to customers. A spoofed phone number hides the actual number the text is coming from and displays a number from a trusted source, like your bank.

The text claims that your debit card has been used to make a purchase and if you do not recognize the transaction, you need to call their fraud prevention helpline. A phone number is provided for you to call.

Warning, this is not a legitimate bank phone number!

Because the incoming text looks like it's from your bank, people are falling for this. If you do call the number provided in the text, the fraudster will answer the phone.

They will then ask you to confirm your sensitive banking details. This would allow the scammer to steal money from your account.

Claire Pearson of the U.K. is a recent victim of this scam. She received the text, called the number and spoke to the fraudster for nearly half an hour, giving him all the sensitive banking information he asked for.

The scammer ended up draining her bank account of almost $90,000. When Pearson reported the fraud to her bank, her claim was denied. The bank said that it was not at fault in this incident because Pearson willingly divulged personal, security information so it would not accept responsibility for the account losses.

This scam is not limited to the U.K. It's also happening right here in the U.S.

Smishing scams are relatively new. Here are some suggestions to defend against them:

How to avoid a smishing scam:

- Phone number - If you receive a text or email claiming to be from your bank, do *NOT* call the phone number that is provided. Whenever you need to discuss banking details, always call the number that is printed on the back of your debit or credit card. That way you know the number is legit and you're not going to be scammed.
- Security details - You should *NEVER* reveal your security details like your full passwords or PIN code over the phone. A bank will never ask for your online account password over the phone. They might ask you to answer a preset security question, which is fine, but never your password.
- Be vigilant - Never assume that a text message or email is genuine. Scammers can spoof phone numbers and email addresses to make them look official. Don't click on links within these messages, always type the website address into your browser or call the phone number located on the back of your card.
- Trust your instincts - If a text or email seems suspicious, delete it immediately. Follow up by calling the company using the trusted phone number on the back of your card.
- Take your time - If you receive a call from someone claiming to be from your bank, don't let them rush you into giving them sensitive information. The incoming number could have been spoofed and a scammer might be on the line. Just tell them that you need a moment and you will call them back. Then call using the phone number that you know is correct.
- Don't feel pressured - If the person calling is pressuring you to give them sensitive data, stay calm and refuse. Just hang up the phone and call the company's trusted number to follow up with the issue.

5. PHISHING CALL SCAM

Do you remember us telling you about a group of hackers demanding ransom from Apple? The "Turkish Crime Family" claimed to have gained access to a massive cache of iCloud and Apple email accounts. If true, this would have allowed the hackers to wipe everything from the victims' gadgets remotely and reset their iCloud accounts.

Now, a new scam has popped up piggybacking on the hackers' threat. People are receiving phone calls from swindlers pretending to be from Apple support. The scammer tells the victim that the iCloud has been hacked and they need to verify their account details.

Warning, this is a scam!

Victims receive an automated message claiming to be from Apple support and are told that their iCloud account has been hacked. They're then redirected to a live person who is supposed to help take care of the issue.

Once on the line, the victim is asked for personal information and credentials to log into their Apple accounts. Some victims have even been asked to pay a fee to have antivirus software installed on their gadget. To make matters worse, it's not antivirus software that they're paying for, it's malware. Yikes!

This phone scam is another type of phishing attack. If you receive one of these calls you need to immediately *hang up!*

You also need to be prepared for the criminal to make several attempts at tricking you. Victims say they received the same call multiple times in a row before the scammer gave up.

An important thing to remember is that Microsoft and Apple will *never* call you to warn of a security problem. This is something you should always remember and be sure to tell people you know.