Mobile Banking App is HERE!

UNION BANK

March 2024

National Slam the Scam Day is March 7, 2024

National "Slam the Scam" Day is designated by Social Security's Office of the Inspector General to raise awareness of government imposter scams, which continue to spread across the United States. Slam the Scam Day is Thursday, March 7, 2024, as part of National Consumer Protection Week, which takes place this year from March 3-9.

Don't let scammers catch you unaware of their malicious tricks and schemes. Scammers are counting on you being uninformed of their deceptive tactics so that you will fall prey to their ruses. Don't let it happen. Join the Social Security Administration on National Slam the Scam Day, to help raise awareness and prevent scammers from succeeding in their crimes. National Slam the Scam Day is an initiative created in 2020 to raise public awareness to combat Social Security-related scams.

In 2022, it expanded to include other government imposter scams as reported losses from consumers climbed to more than $446 million in 2021. According to the Federal Trade Commission, reported losses for 2022 are nearly $509 million. SSA OIG partners with other government agencies, non-profit organizations, and the private sector to increase awareness about how to spot government imposter scams and avoid becoming a victim. Consumer awareness is the most effective method of deterring these crimes, therefore, Slam the Scam Day is held annually as part of the Federal Trade Commission's National Consumer Protection Week, (NCPW).

In a government imposter scam, someone claims to be an SSA, or another government employee, and may ask for personal information, demand payment, or make threats. These scams primarily use the telephone, but scammers may also use email, text messages, social media, or U.S. mail.

Tips for spotting scams is a critical component because it's important to keep consumers aware of current trends and past behavior patterns of the scammers. SSA

Continued on Page 2

EQUAL HOUSING LENDER Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
By Appointment Only

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

OIG provides resources on its website and posts tips and warnings on its social media platforms. SSA OIG urges everyone to be cautious of any contact supposedly from a government agency telling you about a problem you don't recognize and provides the following tips.

Real government officials will NEVER:

- Threaten you with arrest or legal action because you don't agree to pay money immediately.
- Suspend your Social Security number.
- Claim to need personal information or payment to activate a cost-of-living adjustment (COLA) or other benefit increase.
- Pressure you to take immediate action, including sharing personal information.
- Ask you to pay with gift cards, prepaid debit cards, wire transfers, cryptocurrency, or by mailing cash.
- Threaten to seize your bank account.
- Offer to move your money to a "protected" bank account.
- Demand secrecy.
- Direct message you on social media.

SCAM ALERT

Watch out! Scammers target everyone.

Recognize scammers. They may:

- PRETEND to be from an agency or organization you know.
- Say there's a PROBLEM or promise a prize.
- PRESSURE you to act immediately.
- Tell you to PAY in a specific way.

Do not give scammers money or personal information – Ignore them!

How to avoid a scam:

- Remain calm. Talk to someone you trust.
- Hang up or ignore the message. DO NOT click on links or attachments.
- Protect your money. Criminals will insist that you pay in a hard-to-trace manner, such as with a gift card, prepaid debit card, cryptocurrency, wire transfer, money transfer, or by mailing cash.
- Protect your personal information. Be skeptical of a contact you didn't initiate.
- Spread the word. Share your knowledge of Social Security-related scams. Post on social media using the hashtag #SlamtheScam to share your experience and warn others. Visit ssa.gov/scam for more information. Please also share with your friends and family.

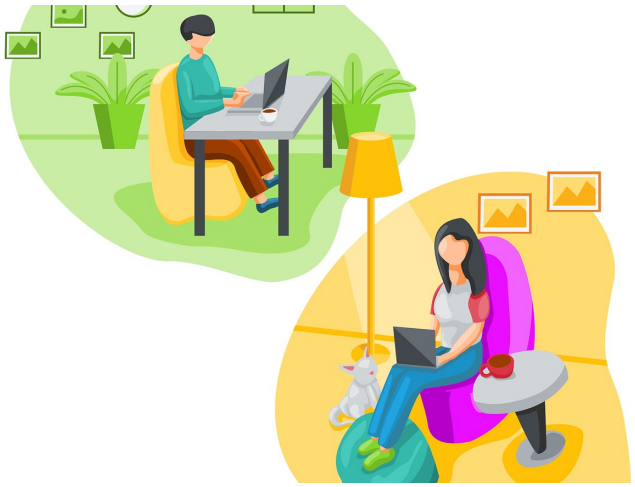
Additional resources can be found at https://www.ssa.gov/scam/resources.html.

The public is encouraged to report Social Security-related scams and fraud online at https://secure.ssa.gov/ipff/home.

Other government imposter scams may be reported to the Federal Trade Commission https://www.ftc.gov/scams.

Sources/Credit:
Article:
Social Security Administration
Images:
Image by Mohamed Hassan from Pixabay,
Image by Cliff Hang from Pixabay,
Attribution: Pixabay, Pixabay Content License Summary

Best Practices for Securing Your Home Network



Don't be a victim! Malicious cyber actors may leverage your home network to gain access to personal, private, and confidential information. Help protect yourself, your family, and your work by practicing cybersecurity-aware behaviors, observing some basic configuration guidelines, and implementing the following mitigations on your home network, including:

- Upgrade and update all equipment and software regularly, including routing devices
- Exercise secure habits by backing up your data and disconnecting devices when connections are not needed
- Limit administration to the internal network only

Recommendations for device security

Electronic computing devices, including computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars, and other “Internet of Things” (IoT) devices must all be secured to reduce the risk of compromise. Most home entertainment and utility devices, such as home monitoring systems, baby monitors, IoT devices, smart devices, Blu-ray™ players, streaming video players, and video game consoles, are capable of accessing the Internet, recording audio, and/or capturing video. Implementing security measures can ensure these devices don’t become the weak link in your home protection.

Upgrade to a modern operating system and keep it up-to-date

The most recent version of any operating system (OS) contains security features not found in previous versions. Many of these security features are enabled by default and help prevent common attack vectors. Increase the difficulty for an adversary to gain privileged access by using the latest available and supported OS for desktops, laptops, and smart devices.

Secure routing devices and keep them up-to-date

Your Internet Service Provider (ISP) may provide a modem/router as part of your service contract. To maximize administrative control over the routing and wireless features of your home network, consider using a personally owned routing device that connects to the ISP-provided modem/router. In addition, use modern router features to create a separate wireless network for guests, for network separation from your more trusted and private devices.

Implement WPA3 or WPA2 on the wireless network

To keep your wireless communications confidential, ensure your personal or ISP provided WAP is capable of Wi-Fi Protected Access 3 (WPA3). If you have devices on your network that do not support WPA3, you can select WPA2/3 instead. This allows newer devices to use the more secure method while still allowing older devices to connect to the network over WPA2.

Implement wireless network segmentation

Leverage network segmentation on your home network to keep your wireless communication secure. At a minimum, your wireless network should be segmented between your primary Wi-Fi, guest Wi-Fi, and IoT network. This segmentation keeps less secure devices from directly communicating with your more secure devices.

Employ firewall capabilities

Ensure that your personally owned routing device supports basic firewall capabilities. Verify that it includes network address translation (NAT) to prevent internal systems from being scanned through the network boundary.

Leverage security software

Leverage security software that provides layered defense via anti-virus, anti-phishing, anti-malware, safe browsing, and firewall capabilities. The security suite may be built into the operating system or available to install as a separate product on computers, laptops, and tablets.

Protect passwords

Ensure that passwords and answers to challenge questions are properly protected since they provide access to personal information. Passwords should be strong, unique for each account, and difficult to guess.

Safeguard against eavesdropping

Be aware that home assistants and smart devices have microphones and are listening to conversations, even when you are not actively engaging with the device. If compromised, the adversary can eavesdrop on conversations. Limit sensitive conversations when you are near baby monitors, audio recording toys, home assistants, and smart devices. Consider muting their microphones when not in use. For devices with cameras (e.g., laptops, monitoring devices and toys) cover cameras when you are not using them. Disconnect Internet access if a device is not commonly used, but be sure to update it when you do use it.

Exercise secure user habits To minimize ransomware risks, back up data on external drives or portable media. Disconnect and securely store external storage when not in use.

Sources/Credit:
Articles:
U.S. Department of Defense
Image:
Image by Arivle One from Pixabay;
Attribution: Pixabay, Pixabay Content License Summary