ACCESSbank®

Digital Banking Safety: Scam Cheat Sheet

Scam and Fraud Definitions

Account Takeover

When scammers take over bank, credit card or government benefit accounts with stolen information; one of the most common types of identity theft.

Malware

Software created to damage, disrupt or gain unauthorized access into someone else's computer system.

Spoofer - Imposter Scam

The act of someone impersonating a trusted company or person in order to access sensitive information.

Spam

Unwanted messages sent to many individuals via text or email.

Vishing

A type of fraud where scammers leave voice messages pretending to be bank reps or other reputable companies in order to gain personal information from their targets.

Smishing

A type of fraud where scammers send text messages pretending to be bank reps or other reputable companies in order to gain personal information from their targets.

Phishing

A type of fraud where scammers send emails pretending to be bank reps or other reputable companies in order to gain personal information from their targets.

Recognize & Avoid **Phishing**

Report Scams: https://reportfraud.ftc.gov

What is Phishing?
A type of fraud where scammers send emails pretending to be bank reps or other reputable companies in order to gain personal information from their targets.

What to know about phishing scams

Scammers like to try to gain your trust by pretending to be a company or someone you know or that seems trustworthy. They want you to click on a link and trick you into giving them personal or account information.

23%

Scammers try to steal your identity or money by sending official-looking email asking for sensitive personal information. 23% of people open phishing email.

To stay safe, keep your computer anti-virus software up to date, use multi-factor authentication (or an additional step for verification) like a text with a code, and make sure to change your passwords often.

Digital Banking Safety: Scam Cheat Sheet

Recognize & Avoid **Imposter Scams**

Report Scams: https://reportfraud.ftc.gov

What is an Imposter Scam?
Someone poses as a person, agency or business that you likely trust, in order to trick you into sending them money.

What to know about imposter scams

These scams can start with an email, text message, or a phone call. The scammer will pretend to be a government official, familiar business, computer repair person, bail bondsman, hospital, or your financial institution – and try to convince you to give up money or personal information.

40%

Scammers can try to get your money from a varietiy of transaction types such as wire transfers, purchasing gift cards and lotteries. 40% of the time posers appear to be government agents such as the IRS, Social Security and Medicare.

To stay safe, be suspicious and never give personal information to anyone over the phone, in response to an email, or text message. Verify the contact from a separate source like a bill or phone directory. Never let anyone take over your computer or give them passwords – never share one-time passcodes unless you intitiate the call.

Recognize & Avoid **Malware**

Report Malware: https://www.ic3.gov/Home/ComplaintChoice
Review anti-virus choices from reputable sources such as: PCMag.com, cnet.com, forbes.com

What is Malware?
Software developed by scammers or "hackers" to steal data and damage computers. Some examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

What to know about malware infections

Malicious apps hide in what looks like a real application, especially when they are downloaded from websites or from links in an email, pop-up ad, text message, or chat message instead of an official app store.

40%

The 2 most common ways to get infected by malware are through online and email. Avoid opening email attachments from unkown sources. When online, you are vulnerable. Mobile phones are also attached - so be careful when using public Wi-Fi.

To stay safe, use strong passwords, back up data, avoid clicking pop-up ads. Make sure reputable anti-virus software is installed, turn on firewall. Stick to trusted sources for mobile apps. Make sure to pay attention to warning messages when installing applications – especially if they ask for permission to access your email, contacts, photos or other personal information.

ACCESSbank®

Digital Banking Safety: Scam Cheat Sheet

Recognize & Avoid Vishing

Report Scams: https://reportfraud.ftc.gov
Register with Do Not Call Registry: https://www.donotcall.gov/register.html

What is Vishing?
A type of fraud where scammers send text messages pretending to be bank reps or other reputable companies in order to gain personal information from their targets.

What to know about vishing scams

Vishing uses a phone call to get you to share personal information – financial details, account numbers and passwords. Scammers can place hundreds of phone calls at a time using VoIP and can spoof the Caller ID to make it look like a trusted source like your bank.

Scammers use schemes such as compromised bank or credit cards, unsolicted loan or investment offers, fake Medicare or Social Security issues, IRS tax threats and utility interruptions to gain personal and financial data.

To stay safe, be leery of a frantic sense of urgency from any caller. Hang up and call back using a number verified from another source like a bill. Don't pick up the phone – simply let it go to voice mail. If it is legitimate, you can call back. Hang up the moment you suspect anything, don't press buttons or respond to prompts.

Recognize & Avoid Smishing

Report Fraudulent Text Messages: dial 7726 (SPAM) from your phone
Every major mobile carrier in the US has banded together
to create a fraud text reporting service.

What is Smishing?
A type of fraud where scammers send emails pretending to be bank reps or other reputable companies in order to gain personal information from their targets.

What to know about smishing scams

Scammers will send you a text asking you to click on a link that will redirect you to a fake website to collect information – these may look identical to a familiar-looking webform, delivery notice, fake bill or website that will try to download malware.

Less than 35% of the population knows what Smishing is – Smishing is one of the easiest ways for hackers to steal user data because we are so glued to our phones and the user is literally giving the scammer all their information.

To stay safe, don't follow links from suspicious texts without verifying the source. **Never** provide personal information via text. **There are numerous legitimate text notifications informing you about things like deliveries, health information, and even suspicious account activity.** If you receive a message that urges you to act via SMS, verify the message. For example, using a separate source to verify the number. Call the company and ask if they sent you a message.

ACCESSbank®

Digital Banking Safety: Scam Cheat Sheet

Recognize & Avoid **Account Takeover**

Report Identity Theft and Start a Recovery Plan:
https://www.identitytheft.gov/#/

What is Account Takeover?
When scammers take over bank, credit card or government benefit accounts with stolen information, and one of the most common types of identity theft.

What to know about account takeovers

Account Takeovers (ATOs) fraud isn't new, but it is growing. Identity theft is at an all-time high. Fraudsters can easily purchase passwords and log in credentials on the dark web for just a few bucks. Scammers gain access to an account and make slight account modifications, such as password changes to gain control.

22% of U.S. adults have been victims of account takeover. With stolen account information—usernames, passwords, email and mailing addresses, bank account routing information and Social Security numbers—scammers can open accounts, make large purchases, even forge a full-blown attack on a person's identity from financial accounts to social media accounts.

To stay safe, create strong passwords and change them often; use multifactor authentication when available; place fraud alerts or credit freezes with all three credit bureaus; consider identity theft protection. Watch account activity and keep good records. Report any suspicious activity to the company or agency involved.

Recognize & Avoid **Spam**

Report Spam: https://www.justice.gov/doj/spam

What is Spam? *(Stupid Pointless Annoying Malware – Monty Python)*
Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

What to know about spam

Spammers use email, text, phone calls and snail mail to send bulk unwanted messages. A lot of these are marketing messages suggesting unsolicited goods, but they can also include malicious types of spam messages spreading malware, or trying to trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.

Email spam filters catch a lot of these messages, and phone carriers often warn you of a "spam risk" from unknown callers. Whether it is email or another type of communication, spam can include phishing, spoofing, tech support scams, event scams, advance fees, too-good-to-be-true jobs or easy ways to pocket some cash.

To stay safe: learn to spot phishing; beware of links and opening attachments; look for grammatical errors; and any communication asking you for missing or personal information. If you do not know the sender, do not open the email! Report all suspicsious email as spam.