



E-mail Scams, Spoofing, Caller ID and Spoofing, Phishing, Texts, and Pop-ups

Phishing e-mails often use official-looking logos and links to trick you. Typically phishing e-mails contain a link to click on an attachment or a file to download. Don't click on any links, open any attachments or download any files. This is one way that you become vulnerable. The scammer is looking for passwords, banking information, social security number, mother's maiden name, date of birth and more.

Top 5 clues to spot an e-mail scam:

1. Check the spelling Scammers are notorious for their lack of basic spelling and grammar skills. Look out for misspelled words and incomplete or awkwardly written sentences in the e-mail. An e-mail that is supposedly from a reputable and well-known organization generally will not contain misspells, especially the name of the organization .
2. Check who signed it An e-mail from a legitimate business may be signed with a person's name and contact information. If an e-mail signs off with something vague, such as "Customer Support," be wary.
3. Does the e-mail scream at you in all caps or have lots of !!!!! at the end? Beware of e-mails that try to get your attention by using all capital letters, especially in the subject line, or that try to scare you with lots of exclamation marks. Using all caps has long been viewed as online shouting, which just isn't done. The authors of scam e-mails tend to write over-the-top and very emotional content. Also, keep an eye out for warnings, such as "Urgent!", "Danger!", "3rd Attempt Declined", "IMPORTANT-PLEASE READ", or "Your account has been temporarily locked!!".
4. The e-mail has an executable attachment Never download an attachment unless you are sure it's legitimate. A favorite ploy of scammers is to send e-mails that look like someone you know sent it to you. Don't be fooled by the sender's name. Always verify that the attached file does not contain a virus. You can do this by running a scan or checking with the sender whether it is a legitimate e-mail.
5. The e-mail has a link to a website Since people have become more aware that they shouldn't download attachments from strangers, scammers have become smarter in the way they try to steal personal information. Instead of attaching a file, they include a clickable link to a website where you might be asked to provide personal information. For example, you might receive an e-mail that appears to be from your bank offering you a very low interest rate on a mortgage or home equity loan. If you click on the link, it could ask your name, bank account number and online banking password to get onto the site. Don't ever provide this information if you have reached the site by clicking a link in an e-mail. BankFIRST will NEVER send you an e-mail requesting confidential information.

One final word of advice: Never, ever respond to a spam e-mail. By doing so, you confirm that your e-mail account is active, and you'll likely be flooded with more spam.

E-mail Spoofing

E-mail spoofing is the forgery of an e-mail header so the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an authentication mechanism. To send spoofed email, senders insert commands in headers that will alter message information. It is possible to send a message that



appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed e-mail appearing to be from you with a message that you didn't write. Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks. For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes. BankFIRST will NEVER send you an e-mail requesting confidential information.

Caller ID and Spoofing

Background

Caller Identification, or "Caller ID," allows you to identify a caller before you answer your telephone. It is sometimes offered as an optional service by landline and wireless telephone companies. A caller's number and/or name are displayed on your phone (if your phone has this feature). Some phone and cable companies that provide phone service even offer widgets that allow you to see caller ID displayed on your TV or computer screen.

Using a practice known as "caller ID spoofing," enables the service to become susceptible to fraud. Callers can deliberately falsify the telephone number and/or name relayed as the Caller ID information to disguise the identity of the calling party. For example, identity thieves who want to collect sensitive information such as your bank account or other financial account numbers, your social security number, your date of birth or your mother's maiden name, sometimes use caller ID spoofing to make it appear as though they are calling from your bank, credit card company, or even a government agency.

Tips for Consumers

- Don't give out personal information in response to an incoming call. Identity thieves are clever; they often pose as representatives of banks, credit card companies, creditors, or government agencies to get people to reveal their account numbers, social security numbers, mother's maiden names, passwords and other identifying information.
- If you get an inquiry from a company or government agency seeking personal information, don't provide it. Instead, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to find out if the entity that supposedly called you actually needs the requested information from you.
- Please let the FCC know about ID spoofers by calling 1-888-CALL-FCC or filing a complaint at www.fcc.gov/complaints.

Phishing

The term "phishing" - as in fishing for confidential information - refers to a scam that encompasses fraudulently obtaining and using an individual's personal or financial information. This is how it works:

- A consumer receives an e-mail which appears to originate from a financial institution, government agency, or other well-known/reputable entity.
- The message describes an urgent reason you must "verify" or "re-submit" personal or confidential information by clicking on a link embedded in the message.
- The provided link appears to be the website of the financial institution, government agency or other wellknown/ reputable entity, but in "phishing" scams, the website belongs to the fraudster/scammer.
- Once inside the fraudulent website the consumer may be asked to provide social security number, account numbers, passwords or other information used to identify the consumer, such as the maiden name of the consumer's mother or the consumer's place of birth.



Enjoy the difference.

- When the consumer provides the information, those perpetrating the fraud can begin to access consumer accounts or assume the person's identity.

Since the early 2000's criminals have been using the FDIC, IRS and various government agency's name and reputation to perpetrate various "phishing" schemes. It is important to note that your bank or any government agency will not ask you to reveal any confidential information.

If you suspect an e-mail or website is fraudulent, please report this information to your bank, company or government agency, using a phone number or e-mail address from a reliable source. Example: If your bank's web page looks different or unusual, contact your bank directly to confirm that you haven't landed on a copycat website set up by criminals. Also, contact the Internet Crime Complaint Center (www.ic3.gov), a partnership between the FBI and the National White Collar Crime Center.

If you suspect that you have been a victim of identity theft, perhaps because you submitted personal information in response to a suspicious, unsolicited e-mail or you see unauthorized charges on your debit card, immediately contact BankFIRST and, if necessary, close existing accounts and open new ones. A BankFIRST representative will assist you with your account(s). Also contact the police and request a copy of any police report or case number for later reference. In addition, call the three major credit bureaus (Equifax at 888-766-0008, Experian at 888-397-3742 and TransUnion at 800-680-7289) to request that a fraud alert be placed on your credit report.

Text Message Scams

Think twice before responding to "urgent" text messages. The FDIC reported a recent scam involved a text message sent to cell phones and smartphones warning bank customers that their debit or credit card had been blocked for security reasons. The message urged users to call a hotline to unblock their card, but instead they reached an automated response system asking for their card number, personal identification number (PIN) and other information. Unfortunately, this was enough information for thieves to create counterfeit cards and commit fraud. Smartphone users are now being targeted by scammers because they almost always have their phone handy and tend to respond to calls and e-mails quickly. The scammers are counting on many of the users not realizing a message is fraudulent until it's too late. Not only that, but fake websites are also harder to spot on a small screen.

Pop-ups

Be on guard against unexpected pop-up windows on websites, including your bank's website. Once you have logged onto a website you should not receive a pop-up asking for personal information. If you get a pop-up window asking for your name, account numbers or other personal information, this is likely a sign that a hacker has infected your PC with spyware. This spyware allows the hacker to troll for enough information to commit identity theft and gain access to your bank account. It's normal for your bank to ask for your login ID and password when you first log in. The bank may also ask you to answer a "challenge question" if you want to reset your password or start using a new computer. However; your bank will not ask you through a pop-up window to type your name or any other personal information. Banks only need detailed personal information when the account is initially opened.