

Learn about . . .

Schemes, Scams and Frauds

Here is a review of the most current prevalent frauds, with some advice for keeping private information secure.

PHISHING

Phishing is the criminal attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email, directing users to enter personal financial details at a fake website whose look and feel are almost identical to a legitimate one, such as their bank. Even when using server authentication, it may require tremendous skill to detect that the website is fake.

► **Protect yourself** by remembering that your financial institution will never send an email asking for personal information or send you to a special site to “update personal information.” If you do not know the source, delete the email and contact the source yourself to verify and/or report the scam.

VISHING

Vishing is the name for phishing attacks using the telephone. The term is a combination of voice and phishing, and is typically used to steal credit card numbers, bank account numbers and passwords. You might receive a phone call advising you that your credit card has been used illegally, and to call a certain number to “verify” your account number.

► **Protect yourself** by being suspicious of any phone call asking you to provide credit card or bank numbers. Rather than provide the information, contact your bank or credit card company directly to verify the validity of the message.

SMISHING

Smishing is yet another variation of phishing, the name a combination of SMS (Short Message Service, the technology used in text messaging) and phishing. In this scam, the fraudster uses cell phone text messages to lure you to a website... or perhaps to use a phone number that connects to an automated voice response system. The smishing text message typically urges your immediate attention. For example, it might say it is confirming an order for a large computer purchase, and you need to follow the scammer’s directions in order not to be charged for the item. Once you click on the URL or call the phone number, you are asked to provide card numbers, account numbers, PIN numbers, etc.

► **Protect yourself** by assuming that no legitimate business would contact you by text message with a request of this nature. If the message seems credible, use your phone to call Directory Service for the correct phone number, then call customer service and ask about the message.

DEBIT & CREDIT CARD SKIMMING

Debit and Credit Card Skimming attempts to hijack your personal information and your identity by tampering with ATM machines. Fraudsters set up a device that is capable of capturing the debit card magnetic stripe and keypad information from the ATM, then sell this information to criminals who use it to create new cards with your account numbers.

► **Protect yourself** first by reducing your risk at ATMs use machines from institutions you know and trust. A thief has to be able to attach and retrieve a skimming device to use the data it's gathered, which is easier in settings where there's less traffic and no surveillance cameras. Additionally, if you notice a change at an ATM you use routinely, such as a color difference in the card reader or a gap where something appears to be glued onto the slot where you insert your card, that's a warning sign to find another machine.

FAKE CHECK SCAMS

Fake check scams use technology to create realistic cashier's checks. These checks are used by scammers to pay for online purchases or most notoriously, some form of foreign lottery that you are told you won. The scam always involves your accepting the faked cashier's check, which is for more than the purchase price, then you sending the difference is a separate check to the scammer. You keep the worthless fake check... and the scammer keeps your real check (with your real money).

► **Protect yourself** using basic common sense. If you are selling something, insist the buyer pay by traditional means. Remember that if you didn't enter a lottery, you would not win it. And of course, never accept a check for more than the amount due.

ADDITIONAL RESOURCES

www.ftc.gov/idtheft

www.onguardonline.gov

(Source: Financial Education Corporation)