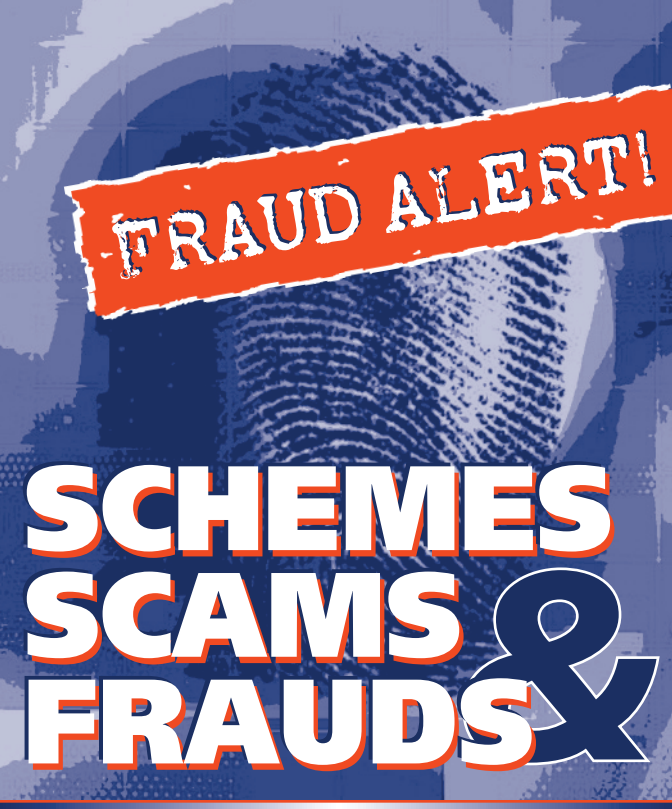

THESE SCAMS CAN COST YOU MONEY:

Phishing...spear phishing...
vishing...smishing...
debit card skimming...
fake check scams

☑ **THE COMMON SENSE PRECAUTIONS INSIDE CAN KEEP YOU SAFE!**

Criminals want to earn their money the easy way—*by stealing yours.*

In the last decade a virtual flood of frauds have arisen using increasingly sophisticated technologies…all aimed at separating you from your money by stealing your personal financial information. It seems that as soon as one devious technique is uncovered, the fraudsters use their ingenuity to devise yet another—each aimed at identity theft or account hijacking. Here is a review of today's **most prevalent frauds,** with some advice for keeping your private information secure.

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.

SPEAR PHISHING is a variation of phishing. With phishing, criminals might send a single, mass e-mail to thousands of people. *Spear*

phishing attacks are customized and sent to a single person at a time. The *spear phishing* email usually contains personal information such as your name or some disarming fact about your employment.

A *spear phishing* email usually includes a link leading to a fake web site that requests personal information. The phony email may contain a downloadable file. They often appear to come from an employer or another seemingly legitimate source. But the file contains malware, and once downloaded to your computer, collects your personal information and transmits it to the criminal.

☑ ***PROTECT YOURSELF*** by understanding that these attacks are usually limited to corporate targets. Nearly all of the *spear phishing* complaints that have been investigated have come from corporate employees. If you receive a suspicious email like this, go directly to HR or to your company's technical people to learn whether the email is legitimate.

☒ **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** 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.

FREE CREDIT REPORTS THE BEST DEFENSE OF ALL

When it comes to guarding against Identity Theft and Account Hijacking, perhaps the most important tool at your disposal is your credit report. It details all of your credit transaction accounts, and will be the first place that unusual charges or entirely new accounts will appear. The good news is that you can monitor your credit report for FREE! But you must exercise this option through specific channels.

Since you are entitled to a free report from each of the three major credit reporting agencies, security experts advise you get a free report from each one every four months. That way, you can keep an eye on your personal account safety year 'round.

To order your free credit report, go to the *only authorized source:*

www.annualcreditreport.com

1-877-322-8228

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** 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** use technology to create realistic cashiers 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 cashiers check, which is for more than the purchase price, then your sending the difference in 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 AT:**

www.ftc.gov/idtheft
www.onguardonline.gov

JOHN MARSHALL BANK

John Marshall Bank
1943 Isaac Newton Square
Suite 100
Reston, VA 20190
(703) 584-0840
www.johnmarshallbank.com