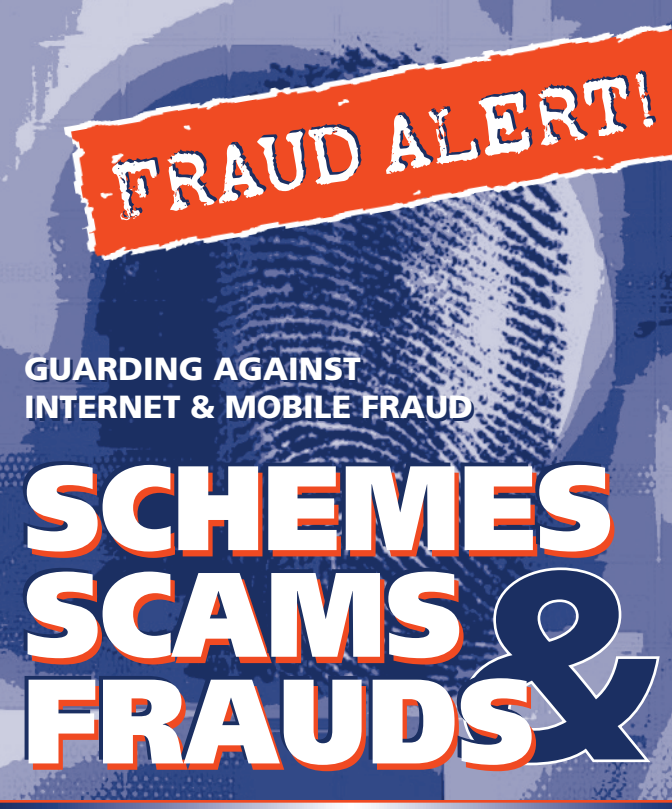

GUARDING AGAINST
INTERNET & MOBILE FRAUD

SCHEMES SCAMS & FRAUDS

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!**

KNOW THE FRAUDS!

In the last decade cyber-frauds have arisen using increasingly sophisticated technologies…all aimed at separating you from your money. 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 steal your personal information through fraudulent emails or smart-phone texts. They are often very believable, luring the victim to a site that asks them to provide (or "verify") personal financial details such as account numbers and social security numbers. A variation is called ***Spear Phishing,*** which are electronic messages that appear to come especially to victims from their employer, usually a large corporation.

> ☑ ***PROTECT YOURSELF:*** Your financial institution will not send emails asking for your personal information—they already have it.

☒ **SMART PHONE TEXTING FRAUDS**

Cyber-security experts often call the text and mobile phone version of phishing ***Smishing,*** playing off the SMS, or Short Message Service, terminology used in text messaging. Smart phone users are being increasingly targeted because these users almost always have their phone handy and tend to respond to texts and emails quickly. They may not realize the message is fake until too late. In addtion, fake Web sites can be harder to spot on a small screen.

☑ ***PROTECT YOURSELF:*** Be careful responding to "urgent" text messages, especially one from your financial institution...call and ask before responding. In all cases with text scams, use the same precautions as you would for a potential phishing scam.

☒ **SPYWARE** is the term used for criminal software that a victim unknowingly loads on a personal computer. Once there, the spyware collects personal information and sends it to the criminal.

☑ ***PROTECT YOURSELF:*** Up-to-date security software is the best defense.

☒ **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. 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.

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

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:*** 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.

HELPFUL HINT: Cyber-criminals often prey on those who are most vulnerable, such as senior citizens or young adults, who may not be as aware of the technical aspects of the threats. Make sure you alert any friends or family members who might be in this category. They'll appreciate it!

RESOURCES

- **Internet Crime Complaint Center:** www.ic3.gov
- **Consumer Fraud (Department of Justice Homepage):** www.usdoj.gov

- **Federal Trade Commission (FTC) Consumer Response Center:** www.ftc.gov
- **Consumer Guides and Protection:** www.usa.gov
- **Financial Fraud Enforcement Task Force:** www.stopfraud.gov
- **On Guard Online:** www.onguardonline.gov