IDENTITY THEFT: A HOW – TO GUIDE

DETER – DETECT – DEFEND

Identity theft occurs when someone uses your personal information, like your credit card number or name and Social Security number, without your permission, to commit fraud or other crimes.

The Federal Trace Commission (FTC) estimates that as many as 10 million people have their identities stolen each year. In fact, you ore someone you know may have experienced some form of identity theft.

It's about the "3 D's" of identity protection – *Deter, Detect, Defend.*

DETER – DETER IDENTITY THIEVES BY SAFEGUARDING YOUR INFORMATION.

- **Shred** financial documents and paperwork with personal information before you discard them.
- **Protect** you Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- **Don't give out** personal information on the phone, through the mail, or over the Internet unless you have initiated contact and know who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit OnGuardOnline.gov for more information.
- **Don't use** an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- **Keep** your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

DETECT – DETECT SUSPICIOUS ACTIVITY BY ROUTINELY MONITORING YOUR FINANCIAL ACCOUNTS AND BILLING STATEMENTS.

Be alert to signs that require immediate attention:

- Mail or bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

Inspect:

- **Your credit report.** Credit reports contain information about you, including what accounts you have and your bill history.
  - The law requires the major nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to give you a free copy of your credit report each year if you ask for it.

- Visit **www.AnnualCreditReport.com** or call 1.877.322.8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Your financial statements.** Review Financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND – DEFEND AGAINST IDENTITY THEFT AS SOON AS YOU SUSPECT A PROBLEM.

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make certain changes to your existing accounts. The three nationwide consumer reporting companies have toll-free number for placing an initial 90-day fraud alert; a call to one company is sufficient:
  - **Equifax:** 1.800.525.6285
  - **Experian:** 1.888.EXPERIAN (397.3742)
  - **TransUnion:** 1.800.680.7289

  Placing a fraud alert entitles you to free copies of your credit reports. Review your credit reports for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- **Close accounts.** Close any accounts that have been tampered with or established fraudulently.
  - Call the security or fraud departments for each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
  - Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
  - Get written verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of your conversations about the theft.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- **Report your complaint to the Federal Trade Commission (FTC).** Your report helps law enforcement officials across the country in their investigations.
  - **Online:** ftc.gov/idtheft
  - **By Phone:** 1.877.ID.THEFT (438.4338) or TTY, 1.866.653.4261
  - **By Mail:** Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

Should you have any questions regarding any of the above information or if you or someone you know has been a victim of identity theft and you need some guidance please call your Fraud Coordintor and/or your Security Officer.

IDENTITY THEFT: A HOW – TO GUIDE

DETER – DETECT – DEFEND

WHAT IS PHISHING?

WHAT WOULD YOU DO...

[Scenario] You receive an email from info@ATMcardsource.com. The email states the following:

"Dear John Q. Customer:

Enclosed is your new PIN number to your ATM/Check card. In order to activate this new PIN and continue using your ATM/Check card, you will need to call us at 1.800.498.4338 or email us at ATMPIN@yahoo.com and provide us with the following:

1. *Name*
2. *SSN*
3. *Account Number / Card Number*
4. *Date of Birth*

Please respond to this email as soon as possible to avoid any unnecessary interruption in service. We look forward to serving you and your banking needs and we appreciate your business.

Customer Service Department
ABC Bank"

WOULD YOU RESPOND TO THIS EMAIL OR DELETE IT IMMEDIATELY?

"In computing, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging, and often directs users to enter details at a website, although phone contact has also been used. Phishing is an example of social engineering techniques used to fool users. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical measure. Phishing is when a fraudster sends you an email or link, claiming to be from a legitimate company. They'll often send you to a fake website they've created, and trick you into entering your password and personal information. You're then an easy target for account/ID Theft." (http://wiki.answers.com/Q/What_is_phishing)

Examples of a trustworthy entity are:

1. A government agency
2. Financial Institution

3. Internet Service Provider (ISP)
4. Internet-based company or any agency or business your trust and/or do business with

Like the scenario above, "a phishing email will either entice you with the promise of money or appeal to your desire to protect your personal information by claiming that your account has been compromised. You will be advised to click on a link in the email in order to receive money or to provide information in order to secure or re-activate your account. The financial enticement or the advice to follow a link and provide additional information in order to secure or re-activate your account is the bait the cybercriminal dangles before you – hence the term phishing." (http://www.insideidtheft.info/internetsecurity.aspx?gclid=CIy61p-PipkCFQO5GgodkQULlg)

"By taking the bait and clicking on the link in a phishing email, you are exposed to at least tow risks:

1. Clicking on any link in a phishing email is that you will be redirected to a web site that will look similar or identical to the web site the cybercriminal is impersonating. Once at the site, you will be directed to provide personal information that will allow the identity thief or cybercriminal to steal that personal information and use it for financial fraud or other crimes.
2. Clicking on any link in a phishing email is that you will be activating the execution and installation of a virus that will be surreptitiously installed on your computer. The virus may steal the personal information store don your computer by transmitting the personal information to the identity thief or cybercriminal who sent you the phishing email. The virus may also take over your computer and turn it into part of a botnet (malicious software robot network) designed to transmit other virus laden emails to thousands of other computers around the world." (http://www.insideidtheft.info/internetsecurity.aspx?gclid=CIy61p-PipkCFQO5GgodkQULlg)

HOW DO I AVOID BECOMING AN IDENTITY THEFT VICTIM AS THE RESULT PHISHING?

1. "Never trust an email you didn't request that directs you to provide information in order to obtain a benefit or to secure or re-activate an account.
2. If you do open an email that requests personal or financial information from you, never lift-click on a link in the email."

(http://www.insideidtheft.info/internetsecurity.aspx?gclid=CIy61p-PipkCFQO5GgodkQULlg)

ALWAYS REMEMBER: "No reputable business or agency will send you an unsolicited email requesting personal or financial information from you. If you believe the email might be legitimate, contact the sending business or agency either by using a web address you've previously bookmarked, one that you obtain independently from the email or by calling a phone number using a listing obtained independently of the email." (http://www.insideidtheft.info/internetsecurity.aspx?gclid=CIy61p-PipkCFQO5GgodkQULlg)

REPORTING A PHISHING EMAIL:

"The anti phishing working group maintains a list of phishing scam emails and websites to help people identity and avoid being scammed in the future.

The anti phishing working group will review the message and any websites to which it links, and post it to the Phishing Archive on the anti phishing working group website.

1. Create a new email to reportphishing@antiphishing.org
2. Drag and drop the phishing email from your inbox onto this new email message
3. Do not use "forward" if you can help it, as this approach loses information and requires more manual processing.

(http://www.insideidtheft.info/report-phishing.aspx)