Scams and Fraud

HOW TO RECOGNIZE THEM AND WAYS YOU CAN PROTECT YOURSELF

PRESENTED BY THE CRIMINAL INVESTIGATIONS DIVISION,

MORGANTON DEPARTMENT OF PUBLIC SAFETY

FRAUD FACTS

- Annually, fraud costs US citizens an estimated $80+ billion…or $950+ per US family.

  -National Insurance Crime Bureau

- 30.2 million people reported being victims of fraud in 2007 (13.5% of the entire US population).

  -Federal Trade Commission, 2007. (www.ftc.gov/opa/2007/10/fraud/shtm)

- In 2008,identity theft fraud complaints were highest in the 20-29 year old age group.

  -Consumer Sentinel Network. January 1-December 31 2008.

- From 2000 to 2008, fraud complaints rose nearly 400% (from 325,519 to 1,233,370) but 63% of victims DID NOT report the fraud to law enforcement.

  -Consumer Sentinel Network

TYPES OF SCAMS

- Internet frauds/scams: Online auction schemes such as fake or dishonest EBay sellers, Nigerian money offers, lotteries, advanced loan offers, fake checks/money order offers and work-at-home plans. ***Phishing*** is a mainstay of Internet scam success.
- Telemarketing frauds: Prizes and sweepstakes scams, scholarships and grants offers, magazine sales, credit card offers. This type of fraud alone costs an estimated $40 billion per year in losses.
- Other types of fraud/scams include
  - Offers of home repair for a greatly reduced price, without a contract, or making advanced payments for future work.
  - Calls saying you have won something of value when you've not entered any contests or drawings.
  - Calls threatening you with severe or immediate legal action

<u>**These are just a few of the many scams out there**</u>

What is PHISHING?

- ***Phishing*** occurs when someone in cyberspace (on the Internet) tries to trick you into giving them your personal information.
  - Emails that ask for your information (name, date of birth, Social Security number, bank name, bank account numbers, credit card name, credit card numbers, user names and passwords) are usually scams. Your bank and credit card company ALREADY HAVE THIS INFORMATION.

RECOGNIZING PHISHING

- **Fake online links.** Always check where a link is going before you click on it. Move your mouse over the link and look at the URL in your browser/status bar.
- **Emails that appear to be websites.** Some emails will look like websites to trick you into entering your personal information.
- **Poorly written text.** Scams often have misspelled words and incorrect grammar.
- **Unsafe Internet sites.** The term ***https*** should always precede any web address where you enter personal information. The s means the website is secure.

IT'S PROBABLY A SCAM…

- If you "win" something (a prize, money, a cruise, etc) when you did not enter a contest;
- If it requires you to put anything in your bank account and then make a withdrawal to send to someone;
- If you have to pay money in advance in order to receive a prize, money or other thing of value;
- If you get any offer from someone you don't know, especially if it comes from outside the US;
- If you get any offer you did not ask for;
- If the offer asks you to enter or verify your personal information;
- If the offer asks you for your bank name, bank account number, a "voided" or blank check, or credit card name and number.

IT'S PROBABLY A SCAM…

- If the email or contact requires IMMEDIATE action on your part;
- If there are threats of immediate criminal action against you;
- If you get a check for a large amount of money you are not owed, you haven't earned or don't know who is sending it;
- If an email or offer has misspellings, poor grammar or gaps in logic;
- If you back out of an Internet deal you previously agreed to and start getting nasty calls from the other party, usually someone who says he or she is a "supervisor" of the person you initially made the deal with.

HOW TO PROTECT YOURSELF

- Pay close attention to your bills and guard your mailbox;
- Mail bills by putting them in a secure post office box rather than leaving them in your mailbox with the flag up;
- Be VERY careful about giving out your personal information, especially over the telephone or Internet;
- Check your bank statements and credit report regularly;
- Stop pre-approved credit card offers;
- Keep watch on your purse, wallet and checkbook;
- **DO NOT** keep PIN numbers with your financial cards;
- Shred mail and other papers containing your personal information.

WHAT TO DO IF YOU BECOME A VICTIM

- **Immediately** notify your bank or credit card company if your wallet, purse, checks or credit/debit cards are stolen;

- Have the bank put a "stop payment" on your credit/debit cards and checks if they are stolen;

WHAT TO DO IF YOU BECOME A VICTIM

- Notify law enforcement and file a police report as soon as possible after contacting your bank and credit card company. Your bank or credit card company may require a police report number.
- Continue to monitor your financial statements and give any suspicious information to the police.

For more information…

- Contact your bank or credit card company
- Consider purchasing commercial identity protection services
- Contact your local law enforcement agency

  Morganton Public Safety 828-437-1211

  Burke Co. Sheriff's Office 828-438-5500
- Read more at the following websites:
  - www.antiphishing.org
  - www.fraud.org
  - www.ftc.gov/sentinel
  - www.nicb.org
  - www.ncdoj.gov
  - www.secretary.state.nc.us