INTRODUCTION

Constantly evolving technology has made our business and social practices more efficient and personal. While communicating with friends and family and accessing information easily makes life more enjoyable, this freedom also makes Internet users more vulnerable to cybercriminals. Cybercriminals exploit the Internet through fraud, unsolicited bulk emails (SPAM), phishing scams, and child exploitation.

FRAUD

The ease and convenience of shopping online has led an increasing number of consumers to purchase goods and services on the Internet. In the process, customers transmit personal information. such as their Social Security Numbers and credit card numbers, through cyberspace. While some of these websites are safe and serve their purpose well, others either do not have the proper security measures or present a fraudulent front with the sole purpose of gaining personal information. In 2007, identity thieves stole $48 billion from financial institutions and $5 billion from individual consumers. Follow these tips to avoid becoming a victim.

Credit Card Fraud

Criminals commit credit card fraud because credit can be obtained quickly and without face-to-face interaction. The thief can then open credit accounts or purchase merchandise with a click of the mouse within seconds of obtaining personal information.

Tips to avoid credit card fraud include:

- Do not provide your credit card number unless the site is secure and reputable. Look for “https:” at the beginning of the web address to make sure the site is secure.
- Look for symbols such as the Better Business Bureau’s Online Reliability and Privacy Seals and the TRUSTe privacy seal.
- Check the website’s privacy policy so you can be assured that you have full control over the uses of your personal information.
- Keep a list of all credit card(s) and account information along with the card issuer’s contact information. If your bill looks suspicious or you lose your credit card(s), contact the card issuer immediately.
- Request a free credit report online at annualcreditreport.com and check for lines of credit that you did not open.
- If you are the victim of fraud, place an initial fraud alert on your credit report with the credit agencies.

Internet Auction Fraud

Internet auction fraud typically occurs in one of two ways: the seller receives the agreed upon funds for the item that was advertised, but fails to deliver the item, or the buyer fails to pay for the item once it has been received.

Tips to avoid Internet auction fraud include:

- Read each auction site's Terms of Use before using.
- Consider what method of payment works best for you, but never send cash.
- Read and print the description of the product, and save all copies of emails between you and the buyer or seller.
- Do not provide your Social Security Number to the seller.

International ("Nigerian") Letter and E-mail Scams

International letter and e-mail scams defraud numerous American consumers each year and result in losses of approximately $100 million annually. International con artists use emails to lure victims by promising confidential business proposals.

Tips to avoid international letter scams include:

- Be skeptical of individuals representing themselves as foreign government officials asking for your help in placing large sums of money in overseas bank accounts. Delete without opening unsolicited emails from these senders.
- Do not believe the promise of large sums of money for your cooperation.
- Do not provide your bank account or credit card numbers to these email senders.

CHILD EXPLOITATION

The same advances in technology that allow our children to expand their realm of knowledge are also leaving them vulnerable to exploitation and harm by computer-sex offenders. It is believed as many as 40,000 sexual predators can be online at any given moment. Internet content filters can protect children while they use the Internet.

Signs your child may be at risk include:

- Your child has a computer with Internet access in his or her room;
- You have a webcam on your computer;
- Child spends large amounts of time online, especially at night;
- Pornography or obscene material is discovered on child's computer;
- You notice a child may receive phone calls from adults (hang-ups when you pick up the phone, adults asking to speak with child); child makes calls to numbers you don't recognize (be aware of who your child speaks with; use re-dial if necessary)
- Child receives mail, gifts, or packages from someone you don't know;
- Child turns monitor off or quickly changes screen on the monitor when you come into the room;
- Child becomes withdrawn from family; and
- Child uses online account belonging to someone else; check your Internet history files or ask your child.

PHISHING

Phishing involves sending unsolicited email in an attempt to capture personal information such as credit card numbers, bank account numbers, social security numbers, passwords, and other information. A typical phishing email might appear as if it is sent from a company you deal with and may say that you must update your account information by clicking on a link in the email. The email will look authentic and have a visible email address claiming to be from a financial institution or other legitimate company, as well as graphics that resemble the company's website. The information you input does not go to the purported company but will be routed to an identity thief.

Tips to avoid phishing include:

- Install anti-virus and anti-spyware software, as well as a firewall on your computer. Keep them regularly updated.
- Do not respond to information in the email. Go to the company's actual website or call the company to ensure that the email is authentic.

TABNABBING

Tabnabbing is a form of a "phishing" scam where a criminal runs a computer program to alter a legitimate website that has been opened on a user's Internet browser. The program, or "script," will find an open and hidden webpage tab on the user's Internet browser and rewrite the webpage behind the tab to mirror the website that the user had initially opened. It will typically seek out sites that ask for personal information such as a login ID and password. When the user returns to the page and enters the information it is redirected to the criminal's computer server.

Tips to avoid tabnabbing include:

- Avoid opening several websites at the same time
- Do not keep numerous websites open for a long period of time
- Close and reopen websites that have been open for a long period of time to ensure they are the correct page.

UNSOLICITED BULK E-MAIL

Unsolicited bulk e-mail, sometimes referred to as "UBE" or "SPAM," is email that is sent for the purpose of selling goods, services, or properties. Commercial UBE advertisements are most often used for multi-level marketing schemes, get-rich-quick schemes, work-at-home schemes, or for questionable products or pornography. Fraudulently sent SPAM violates the criminal laws of Virginia.

Tips to prevent SPAM include:

- If you have doubts about the authenticity of the sender and/or the content, do not respond.

- Get a free email account specifically for newsgroups and registering on websites.
- Do not post your actual email address on your website; spammers have programs that can scan web pages for an email address. Consider using a free web-based account such as AOL, Hotmail, Yahoo, or Gmail.
- Report SPAM to the Federal Trade Commission at ftc.gov.
- Use mail filters. They are not always completely accurate, but they can decrease the number of junk emails you receive.