Online Security and Safety

While the Internet makes many everyday tasks faster and more convenient, like shopping, banking, and communicating on the go, it's important to be safe, secure, and responsible online.

Protect Your Privacy and Security

You can protect your computer and personal data from theft, misuse, and destruction with some basic precautions.

- Scams - Learn how to recognize scams and what you can do to avoid them.
- Computer and online security - Defend yourself against scammers, hackers, and identity thieves by protecting your information and your computer while online. If you are a parent, you should also talk to your kids about being safe and responsible online.

Visit OnGuardOnline.gov for more tips for parents and children on being safe and smart online.

Cybercrime and Internet Fraud

Scam artists in the U.S. and around the world defraud millions of people each year by using the Internet to trick victims into sending money or giving out personal information.

Types of Internet Fraud

Internet crime schemes target victims using various methods.

- **Internet auction fraud -** This scheme involves the misrepresentation of a product advertised for sale on an Internet auction site or non-delivery of merchandise.
- **Credit card fraud -** Through the unauthorized use of a credit/debit card, or card number, scammers fraudulently obtain money or property.
- **Investment fraud -** This is an offer using false claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities.
- **Nigerian letter or "419" fraud -** Named for the violation of Section 419 of the Nigerian Criminal Code, it combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, e-mail, or fax is received by the victim.

Tips for Avoiding Internet Fraud

Preventative measures will assist you in being informed prior to entering into transactions over the Internet.

- **Know your seller -** If you don't know who you're buying from online, do some research.
- **Protect your personal information -** Don't provide it in response to an e-mail, a pop-up, or a website you've linked to from an e-mail or web page.

The Federal Bureau of Investigation (FBI) has additional tips to protect yourself and your family from the various types of Internet fraud. (http://www.fbi.gov/scams-safety/fraud/internet_fraud/)

Report Internet Fraud

If you believe you've been a victim of Internet fraud or cyber crime, report it:

- You can report a cyber scam or threat by filing a complaint with the Internet Crime Complaint Center (IC3). (http://www.ic3.gov/complaint/default.aspx)

Report Cyber Crime

If you believe you have been a victim of an Internet-related crime, you can file a report with these government authorities:

- The Internet Crime Complaint Center (IC3) refers Internet-related criminal complaints to federal, state, local, or international law enforcement.
- EConsumer.gov accepts complaints about online and related transactions with foreign companies.
- The Department of Justice (DOJ) can help you report computer, Internet-related, or intellectual property crime to the proper agency, based on the scope of the crime.

Phishing and Vishing

Phishing is a scam in which you receive a fraudulent e-mail designed to steal your identity or vital personal information, such as credit card numbers, bank account numbers, debit card PINs, and passwords. A phishing e-mail often asks you to verify this type of information. The e-mail may state that your account has been compromised or that one of your accounts was charged incorrectly, but you must click on a link in the e-mail or reply with your bank account number to confirm your identity or protect your account.

Legitimate companies never ask for your password or account number via e-mail. The e-mail may even threaten to disable your account, if you don't reply, but don't believe it. If you receive an e-mail there are several actions you should take:

- Don't click on any links in the e-mail. They can contain a virus that can harm your computer. Even if links in the e-mail say the name of the company, don't trust them. They may redirect to a fraudulent website.
- Don't reply to the e-mail itself. Instead forward the e-mail to the Federal Trade Commission at spam@uce.gov.
- If you believe that the e-mail is valid, contact the company using the phone numbers listed on your statements or in the phone book. Tell the customer service representative about the e-mail and ask if your account has been compromised. You can also contact the company online by typing the company's web address directly into the address bar; never use the links to provided in the e-mail.

- If you clicked on any links in the phishing e-mail or replied with the requested personal information, contact your bank directly to let them know and ask to have fraud alerts placed on your accounts, have new credit cards issued, or set new passwords.

Vishing

Similar to phishing, vishing scammers also seek to get you to provide your personal information. However, instead of using e-mail to request the information, vishing scammers use the phone to make their requests. You may be directed to call a phone number to verify an account or to reactivate a debit or credit card. If you have received one of these calls, report it to the Internet Crime Complaint Center. (http://www.ic3.gov/complaint/default.aspx)

Internet Crime Prevention Tips

Internet crime schemes that steal millions of dollars each year from victims continue to plague the Internet through various methods. Following are preventative measures that will assist you in being informed prior to entering into transactions over the Internet:

AUCTION FRAUD

- Before you bid, contact the seller with any questions you have.
- Review the seller's feedback.
- Be cautious when dealing with individuals outside of your own country.
- Ensure you understand refund, return, and warranty policies.
- Determine the shipping charges before you buy.
- Be wary if the seller only accepts wire transfers or cash.
- If an escrow service is used, ensure it is legitimate.
- Consider insuring your item.
- Be cautious of unsolicited offers.

COUNTERFEIT CASHIER'S CHECK

- Inspect the cashier's check.
- Ensure the amount of the check matches in figures and words.
- Check to see that the account number is not shiny in appearance.
- Be watchful that the drawer's signature is not traced.
- Official checks are generally perforated on at least one side.
- Inspect the check for additions, deletions, or other alterations.
- Contact the financial institution on which the check was drawn to ensure legitimacy.
- Obtain the bank's telephone number from a reliable source, not from the check itself.
- Be cautious when dealing with individuals outside of your own country.

CREDIT CARD FRAUD

- Ensure a site is secure and reputable before providing your credit card number online.
- Don't trust a site just because it claims to be secure.
- If purchasing merchandise, ensure it is from a reputable source.
- Promptly reconcile credit card statements to avoid unauthorized charges.
- Do your research to ensure legitimacy of the individual or company.

- Beware of providing credit card information when requested through unsolicited emails.

DEBT ELIMINATION

- Know who you are doing business with — do your research.
- Obtain the name, address, and telephone number of the individual or company.
- Research the individual or company to ensure they are authentic.
- Contact the Better Business Bureau to determine the legitimacy of the company.
- Be cautious when dealing with individuals outside of your own country.
- Ensure you understand all terms and conditions of any agreement.
- Be wary of businesses that operate from P.O. boxes or maildrops.
- Ask for names of other customers of the individual or company and contact them.
- If it sounds too good to be true, it probably is.

DHL/UPS

- Beware of individuals using the DHL or UPS logo in any email communication.
- Be suspicious when payment is requested by money transfer before the goods will be delivered.
- Remember that DHL and UPS do not generally get involved in directly collecting payment from customers.
- Fees associated with DHL or UPS transactions are only for shipping costs and never for other costs associated with online transactions.
- Contact DHL or UPS to confirm the authenticity of email communications received.

EMPLOYMENT/BUSINESS OPPORTUNITIES

- Be wary of inflated claims of product effectiveness.
- Be cautious of exaggerated claims of possible earnings or profits.
- Beware when money is required up front for instructions or products.
- Be leery when the job posting claims "no experience necessary".
- Do not give your social security number when first interacting with your prospective employer.
- Be cautious when dealing with individuals outside of your own country.
- Be wary when replying to unsolicited emails for work-at-home employment.
- Research the company to ensure they are authentic.
- Contact the Better Business Bureau to determine the legitimacy of the company.

ESCROW SERVICES FRAUD

- Always type in the website address yourself rather than clicking on a link provided.
- A legitimate website will be unique and will not duplicate the work of other companies.
- Be cautious when a site requests payment to an "agent", instead of a corporate entity.
- Be leery of escrow sites that only accept wire transfers or e-currency.
- Be watchful of spelling errors, grammar problems, or inconsistent information.
- Beware of sites that have escrow fees that are unreasonably low.

IDENTITY THEFT

- Ensure websites are secure prior to submitting your credit card number.
- Do your homework to ensure the business or website is legitimate.
- Attempt to obtain a physical address, rather than a P.O. box or maildrop.

- Never throw away credit card or bank statements in usable form.
- Be aware of missed bills which could indicate your account has been taken over.
- Be cautious of scams requiring you to provide your personal information.
- Never give your credit card number over the phone unless you make the call.
- Monitor your credit statements monthly for any fraudulent activity.
- Report unauthorized transactions to your bank or credit card company as soon as possible.
- Review a copy of your credit report at least once a year.

INTERNET EXTORTION

- Security needs to be multi-layered so that numerous obstacles will be in the way of the intruder.
- Ensure security is installed at every possible entry point.
- Identify all machines connected to the Internet and assess the defense that's engaged.
- Identify whether your servers are utilizing any ports that have been known to represent insecurities.
- Ensure you are utilizing the most up-to-date patches for your software.

INVESTMENT FRAUD

- If the "opportunity" appears too good to be true, it probably is.
- Beware of promises to make fast profits.
- Do not invest in anything unless you understand the deal.
- Don't assume a company is legitimate based on "appearance" of the website.
- Be leery when responding to invesment offers received through unsolicited email.
- Be wary of investments that offer high returns at little or no risk.
- Independently verify the terms of any investment that you intend to make.
- Research the parties involved and the nature of the investment.
- Be cautious when dealing with individuals outside of your own country.
- Contact the Better Business Bureau to determine the legitimacy of the company.

LOTTERIES

- If the lottery winnings appear too good to be true, they probably are.
- Be cautious when dealing with individuals outside of your own country.
- Be leery if you do not remember entering a lottery or contest.
- Be cautious if you receive a telephone call stating you are the winner in a lottery.
- Beware of lotteries that charge a fee prior to delivery of your prize.
- Be wary of demands to send additional money to be eligible for future winnings.
- It is a violation of federal law to play a foreign lottery via mail or phone.

NIGERIAN LETTER OR "419"

- If the "opportunity" appears too good to be true, it probably is.
- Do not reply to emails asking for personal banking information.
- Be wary of individuals representing themselves as foreign government officials.
- Be cautious when dealing with individuals outside of your own country.
- Beware when asked to assist in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.
- Be cautious when additional fees are requested to further the transaction.

PHISHING/SPOOFING

- Be suspicious of any unsolicited email requesting personal information.
- Avoid filling out forms in email messages that ask for personal information.
- Always compare the link in the email to the link that you are actually directed to.
- Log on to the official website, instead of "linking" to it from an unsolicited email.
- Contact the actual business that supposedly sent the email to verify if the email is genuine.

PONZI/PYRAMID

- If the "opportunity" appears too good to be true, it probably is.
- Beware of promises to make fast profits.
- Exercise diligence in selecting investments.
- Be vigilant in researching with whom you choose to invest.
- Make sure you fully understand the investment prior to investing.
- Be wary when you are required to bring in subsequent investors.
- Independently verify the legitimacy of any investment.
- Beware of references given by the promoter.

RESHIPPING

- Be cautious if you are asked to ship packages to an "overseas home office."
- Be cautious when dealing with individuals outside of your own country.
- Be leery if the individual states that his country will not allow direct business shipments from the United States.
- Be wary if the "ship to" address is yours but the name on the package is not.
- Never provide your personal information to strangers in a chatroom.
- Don't accept packages that you didn't order.
- If you receive packages that you didn't order, either refuse them upon delivery or contact the company where the package is from.

SPAM

- Don't open spam. Delete it unread.
- Never respond to spam as this will confirm to the sender that it is a "live" email address.
- Have a primary and secondary email address - one for people you know and one for all other purposes.
- Avoid giving out your email address unless you know how it will be used.
- Never purchase anything advertised through an unsolicited email.

THIRD PARTY RECEIVER OF FUNDS

- Do not agree to accept and wire payments for auctions that you did not post.
- Be leery if the individual states that his country makes receiving these type of funds difficult.
- Be cautious when the job posting claims "no experience necessary".
- Be cautious when dealing with individuals outside of your own.

Information gathered from:
https://www.usa.gov/online-safety
https://www.ic3.gov/preventiontips.aspx