

INTERNET CRIME PREVENTION TIPS

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 investment 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 country.

The above tips come from <http://www.ic3.gov>