

ONLINE CRIME PREVENTION TIPS

Tips to Protect You and Your Personal Information

INTERNET CRIME COMPLAINT CENTER'S (IC3) ONLINE CRIME PREVENTION TIPS



SeniorBrigade
A MICHIGAN SENIORS INITIATIVE

AUCTION FRAUD

CREDIT CARD FRAUD

DEBT ELIMINATION

EMPLOYMENT BUSINESS OPPORTUNITIES

IDENTITY THEFT

INVESTMENT FRAUD, PONZI AND PYRAMID SCHEMES

LOTTERIES

PHISHING/SPOOFING

RESHIPING

ROMANCE SCAMS

SPAM

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 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.
- * Consider insuring your item.

CREDIT CARD FRAUD

- * If purchasing merchandise, ensure it is from a reputable source. Do research to ensure legitimacy of the individual or company.
- * Beware of providing credit card information through unsolicited emails.
- * Promptly reconcile credit card statements to avoid unauthorized charges.

ONLINE CRIME PREVENTION TIPS

Tips to Protect You and Your Personal Information

DEBT ELIMINATION

- * Know who you are dealing with - do your research. Contact the Attorney General's Office or the State Corporation Commission to see if there are any registered complaints.
- * Be cautious when dealing with individuals outside your country.
- * Ensure that you understand all terms and conditions of any agreement.
- * Be wary of businesses that operate from P.O. boxes or mail drops.

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 suspicious when the job posting claims "no experience necessary."
- * Do not give your Social Security number when first interacting with your prospective employer.
- * Be wary when replying to unsolicited emails for work-at-home employment.

IDENTITY THEFT

- * Ensure websites are secure before submitting a credit card number.
- * Never throw away credit card or bank statements in usable form.

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

INVESTMENT FRAUD, PONZI AND PYRAMID SCHEMES

- * If the opportunity appears too good to be true, it probably is.
- * Beware of promises to make fast profits.
- * Be wary of investments that offer high returns at little or no risk.
- * Be cautious when you are required to bring in subsequent investors.
- * Do not invest in anything unless you understand the deal.
- * Independently verify the terms of any investment that you intend to make. Beware of references given by the promoter.
- * Do not assume a company is legitimate based on the appearance of the website.
- * Be cautious when responding to investment offers received through unsolicited email.

ONLINE CRIME PREVENTION TIPS

Tips to Protect You and Your Personal Information

LOTTERIES

- * Be wary if you do not remember entering a lottery or contest.
- * Be cautious if you receive a telephone call stating you are the winner of a lottery.
- * Beware of lotteries that charge a fee before delivering your prize.
- * Be wary of demands to send additional money to be eligible for future winnings.
- * Know that it is a violation of federal law to play a foreign lottery via mail or phone.

PHISHING/SPOOFING

- * Be suspicious of any unsolicited email requesting personal information.
- * Avoid filling out forms in email messages that ask for personal information. This could be a phishing scam.
- * Always compare the link in the email to the link that you are actually directed to visit.
- * Log on to the entity's 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.

RESHIPPING

- * Be cautious if you are asked to ship packages to an "overseas home office."

- * Be suspicious if an individual states that his country will not allow direct business shipments from the United States.
- * Do not accept packages you did not order.
- * If you receive packages you did not order, either refuse delivery or contact the company that sent the package.

ROMANCE SCAMS

- * Be cautious of individuals who claim it was destiny or fate and you are meant to be together, or claim a higher power brought you to him/her. They often claim to love you within 24-48 hours.
- * Beware of "suitors" who want your address to send you flowers, candy and teddy bears, often purchased with stolen credit cards.
- * Use online search engines to check the information in a "suitors" profile, look for suspect details, inconsistencies and poor language skills: most romance fraudsters are overseas.
- * Be on guard for controlling, manipulative behavior and sob stories about serious illnesses or lost loved ones that play on your sympathies - no matter how credible they sound.
- * If a "suitor" asks you to wire or send money to them or someone else - even if it's to pay for a face-to-face meeting with you - shut down the "relationship" immediately.

ONLINE CRIME PREVENTION TIPS

Tips to Protect You and Your Personal Information

PLEASE KEEP THESE POINTS IN MIND:

- * Be cautious when dealing with individuals outside of your own country.
- * Beware of providing credit card information through unsolicited emails.
- * Ensure that you understand all terms and conditions of any agreement.
- * Beware when money is required up front for instructions or products.
- * Ensure websites are secure before submitting a credit card number.
- * If the opportunity appears too good to be true, it probably is.
- * Know that it is a violation of federal law to play a foreign lottery via mail or phone.
- * Be suspicious of any unsolicited email requesting personal information.
- * Do not accept packages you did not order.
- * If a "suitor" asks you to wire or send money to them or someone else - even if it's to pay for a face-to-face meeting with you - shut down the "relationship" immediately.



SeniorBrigade
A MICHIGAN SENIORS INITIATIVE

SPAM

Is any unwanted online communication

- * Do not open texts or emails from questionable sources. **DELETE IT!**
- * Never respond to spam. Requesting to be removed from an email list may result in additional spam. Responding notifies spammers that an email address is valid.
- * 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.
- * Use an email filter. Some service providers offer a tool that filters out potential spam into a bulk email folder.
- * Never purchase anything advertised through unsolicited email.

Additional information is available on Internet Crime Complaint Center's (ic3) website at:

<https://www.ic3.gov/default.aspx>