

How To Stay Safe Online

- Information compiled by Tabitha Hawk of Nashville Computer Guru using information from onguardonline.gov and other sites.

This article contains some brief information about malware, viruses that can be read in greater detail in my article "What Is this Spyware".

Overview

Online and Offline worlds are equally crazy, just like in our real world people with malicious intentions along with scammers, Identity thieves and hackers lurk online. How do you navigate the only world and popularity of such sites as craigslist, ebay, facebook and others?

A very common issue that I see as a computer technician is malware, spyware and viruses. Every 10 minutes cyber criminals alter their attack code, virus, worm, Trojan, and other zero-day malware, resulting in typical anti-virus/spyware software (signature-based like a vaccine) only stopping 29% of today's attacks on average. Malware has reached epidemic proportions and is only getting worse.

Out of all computer code released onto the internet today, most appears to be of a malicious nature. According to Symantec sensors in 2008, the release rate of malware and other unwanted software may soon exceed that of legitimate applications. F-Secure follows this up by reporting that just as much malware was released in 2007 as in the past twenty years combined. As the outbreak of malicious software is likely to only get worse, it's important to take every precaution when conducting activities on the internet. I have seen recent statistics indicating that approximately 95% of the world's PCs are infected with spyware. Unfortunately, removal techniques that worked just a year ago are no longer effective in many cases.

Email Scams and Phishing

A very common problem online is spam, scams and phishing. Spam – unsolicited sales pitches – also can be costly, with offers for bogus products and fraudulent promotions. Learn to spot 10 common spam scams and what to do if one shows up in your inbox.

How the Guru Got Taken On A Scam

I keep seeing these weightless blogs that looked legit claiming how they lost weight and started with these free samples of Acai berry and this one site also included something called colon cleanse and I just had to pay \$3.99 postage from each company. With all the promises and positive comments on the blog (which the comment feature was disabled because of spam – legit reason but also should be a flag)

I ordered a free sample and it said that after 14 days you will be shipped a full month supply and be billed for it. Little did I know that the sample just happened to be delivered on the 14th day, I got the "free sample" and the full month supply together on the same day in two different packages.

Knowing that wasn't right I went online and checked my bank account was charged \$3.99 and \$82.99 for the one bottle of Acai berry to look for a phone

number to cancel the auto billing. After calling and calling and getting a busy signal or people that spoke very poor English, they refused to give me credit for anything saying that I had 14 days from the time I placed the order online to cancel the auto billing and the shipping delay was out of there control. Fishy how it happened to arrive on the 14th day exactly. They refused to take the product back even unopened.

The next day the Colon cleanse arrived and my bank account was charged for \$79.99 for the one month of pills for that of what was supposed to be a sample for \$3.99, instead no sample and was charged the full amount. The customer support number was disconnected when I called.

Thankfully I used my debit card and after filing a complaint with my bank, I was refunded the full amount and got a new card number to prevent future charges. In addition to all of this, after taking these pills and feeling no difference and the time spent trying to get this situation solved I learned personally about online safety and being diligent about researching products.

Quick Facts

Some email users have lost money to bogus offers that arrived as spam in their in-box. Con artists are very cunning; they know how to make their claims seem legitimate. Some spam messages ask for your business, others invite you to a website with a detailed pitch. Either way, these tips can help you avoid spam scams:

- Protect your personal information. Share credit card or other personal information only when you're buying from a company you know and trust.
- Know who you're dealing with. Don't do business with any company that won't provide its name, street address, and telephone number.
- Take your time. Resist any urge to "act now" despite the offer and the terms. Once you turn over your money, you may never get it back. In fact a lot of those counters are just animated graphics or they are just scripts on the website that reset each day or every time you load the website. They just want to give you the urgency to get the product before the deadline arrives.
- Read the small print. Get all promises in writing and review them carefully before you make a payment or sign a contract.
- Never pay for a "free" gift. Disregard any offer that asks you to pay for a gift or prize. If it's free or a gift, you shouldn't have to pay for it. Free means free.

Filter Tips: 10 Scams to Screen from Your Email

1. [The "Nigerian" Email Scam](#)
2. [Phishing](#)
3. [Work-at-Home Scams](#)
4. [Weight Loss Claims](#)
5. [Foreign Lotteries](#)
6. [Cure-All Products](#)
7. [Check Overpayment Scams](#)
8. [Pay-in-Advance Credit Offers](#)
9. [Debt Relief](#)
10. [Investment Schemes](#)

While some consumers find unsolicited commercial email – also known as "spam" – informative, others find it annoying and time consuming. Still others find it expensive: They're among the people who have lost money to spam that contained bogus offers and fraudulent promotions.

Many Internet Service Providers and computer operating systems offer filtering software to limit the spam in their users' email inboxes. In addition, some old-fashioned 'filter tips' can help you save time and money by avoiding frauds pitched in email. Spam is annoying and can grow out of control if you respond to any one email, click on any links in the email or give out your email to "email harvester" websites (ie. Scam sites that want your email address)

Here's how to spot 10 common spam scams:

1. The "Nigerian" Email Scam

The Bait: Con artists claim to be officials, businesspeople, or the surviving spouses of former government honchos in Nigeria or another country whose money is somehow tied up for a limited time. They offer to transfer lots of money into your bank account if you will pay a fee or "taxes" to help them access their money. If you respond to the initial offer, you may receive documents that look "official." Then they ask you to send money to cover transaction and transfer costs and attorney's fees, as well as blank letterhead, your bank account numbers, or other information. They may even encourage you to travel to the country in question, or a neighboring country, to complete the transaction. Some fraudsters have even produced trunks of dyed or stamped money to try to verify their claims.

The Catch: The emails are from crooks trying to steal your money or your identity. Inevitably, in this scenario, emergencies come up, requiring more of your money and delaying the "transfer" of funds to your account. In the end, there aren't any profits for you, and the scam artist vanishes with your money. The harm sometimes can be felt even beyond your pocketbook: according to State Department reports, people who have responded to "pay in advance" solicitations have been beaten, subjected to threats and extortion, and in some cases, murdered.

Your Safety Net: If you receive an email from someone claiming to need your help getting money out of a foreign country, don't respond. Forward "Nigerian" scams – including all the email addressing information – to spam@uce.gov. If you've lost money to one of these schemes, call your local Secret Service field office. Local field offices are listed in the Blue Pages of your telephone directory.

2. Phishing

The Bait: Email or pop-up messages that claim to be from a business or organization you may deal with – say, an Internet Service Provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information or face dire consequences. This is very common way identity theft happens but it can also be another avenue for malware.

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

Phishing is a scam where internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

To avoid getting hooked:

- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. Most people get infected from email attachments even though they know the person sending it. After opening up the attachment, your friends might get an email coming from you with an attachment and therefore the cycle continues.
- Forward phishing emails to spam@uce.gov – and to the company, bank, or organization impersonated in the phishing email. You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.
- **If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either.** Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.
- **Area codes can mislead.** Some scammers send emails that appear to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use [Voice over Internet Protocol technology](#), the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card. And delete any emails that ask you to confirm or divulge your financial information.
- **Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.** Some phishing emails contain software that can harm your computer or track your activities on the internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that

recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

A firewall helps make you invisible on the internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- **Be cautious about opening any attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

The Catch: Phishing is a scam where internet fraudsters send spam or pop-up messages to reel in personal and financial information from unsuspecting victims. The messages direct you to a website that looks just like a legitimate organization's site, or to a phone number purporting to be real. But these are bogus and exist simply to trick you into divulging your personal information so the operators can steal it, fake your identity, and run up bills or commit crimes in your name.

Your Safety Net: Make it a policy never to respond to emails or pop-ups that ask for your personal or financial information, click on links in the message, or call phone numbers given in the message. Don't cut and paste a link from the message into your Web browser, either: phishers can make links look like they go one place, but then actually take you to a look-alike site. If you are concerned about your account, contact the organization using a phone number you know to be genuine, or open a new internet browser session and type in the company's correct Web address yourself. Using anti-virus and anti-spyware software and a firewall, and keeping them up to date, can help.

Forward phishing emails to spam@uce.gov and to the organization that is being spoofed.

3. Work-at-Home Scams

The Bait: Advertisements that promise steady income for minimal labor – in medical claims processing, envelope-stuffing, craft assembly work, or other jobs. The ads use similar come-ons: Fast cash. Minimal work. No risk. And the advantage of working from home when it's convenient for you.

The Catch: The ads don't say you may have to work many hours without pay, or pay hidden costs to place newspaper ads, make photocopies, or buy supplies, software, or equipment to do the job. Once you put in your own time and money, you're likely to find promoters who refuse to pay you, claiming that your work isn't up to their "quality standards."

Your Safety Net: The FTC has yet to find anyone who has gotten rich stuffing envelopes or assembling magnets at home. Legitimate work-at-home business promoters should tell you – in writing – exactly what's involved in the program they're selling. Before you commit any money, find out what tasks you will have to perform, whether you will be paid a salary or work on commission, who will pay you, when you will get your first paycheck, the total cost

of the program – including supplies, equipment and membership fees – and what you will get for your money. Can you verify information from current workers? Be aware of "shills," people who are paid to lie and give you every reason to pay for work. Get professional advice from a lawyer, an accountant, a financial advisor, or another expert if you need it, and check out the company with your local consumer protection agency, state Attorney General and the Better Business Bureau – not only where the company is located, but also where you live.

4. Weight Loss Claims (Acai berry is a popular Scam)

The Bait: Emails promising a revolutionary pill, patch, cream, or other product that will result in weight loss without diet or exercise. Some products claim to block the absorption of fat, carbs, or calories; others guarantee permanent weight loss; still others suggest you'll lose lots of weight at lightening speed.

The Catch: These are gimmicks, playing on your sense of hopefulness. There's nothing available through email you can wear or apply to your skin that can cause permanent – or even significant weight loss.

Your Safety Net: Experts agree that the best way to lose weight is to eat fewer calories and increase your physical activity so you burn more energy. Permanent weight loss happens with permanent lifestyle changes. Talk to your health care provider about a nutrition and exercise program suited to your lifestyle and metabolism.

5. Foreign Lotteries

The Bait: Emails boasting enticing odds in foreign lotteries. You may even get a message claiming you've already won! You just have to pay to get your prize or collect your winnings.

The Catch: Most promotions for foreign lotteries are phony. The scammers will ask you to pay "taxes," "customs duties," or fees – and then keep any money you send." Scammers sometime ask you to send funds via wire transfer. Don't send cash or use a money-wiring service because you'll have no recourse if something goes wrong. In addition, lottery hustlers use victims' bank account numbers to make unauthorized withdrawals or their credit card numbers to run up additional charges. And one last important note: participating in a foreign lottery violates U.S. law.

Your Safety Net: Skip these offers. Don't send money now on the promise of a pay-off later.

6. Cure-All Products

The Bait: Emails claiming that a product is a "miracle cure," a "scientific breakthrough," an "ancient remedy" – or a quick and effective cure for a wide variety of ailments or diseases. They generally announce limited availability, and require payment in advance, and offer a no-risk "money-back guarantee." Case histories or testimonials by consumers or doctors claiming amazing results are not uncommon.

The Catch: There is no product or dietary supplement available via email that can make good on its claims to shrink tumors, cure insomnia, cure impotency, treat Alzheimer's disease, or prevent severe memory loss. These kinds of claims deal with the treatment of diseases; companies that want to make claims like these must follow the FDA's pre-market testing and review process required for new drugs.

Your Safety Net: When evaluating health-related claims, be skeptical. Consult a health care professional before buying any "cure-all" that claims to treat a wide range of ailments or offers quick cures and easy solutions to serious illnesses. Generally speaking, a cure all is a cure none. You should google what product, company, etc with the word "scam" or "compliments" (example "acai berry scam"). Research is important.

7. Pay-in-Advance Credit Offers

The Bait: News that you've been "pre-qualified" to get a low-interest loan or credit card, or repair your bad credit even though banks have turned you down. But to take advantage of the offer, you have to ante up a processing fee of several hundred dollars.

The Catch: A legitimate pre-qualified offer means you've been selected to apply. You still have to complete an application and you can still be turned down. If you paid a fee in advance for the promise of a loan or credit card, you've been hustled. You might get a list of lenders, but there's no loan, and the person you've paid has taken your money and run.

Your Safety Net: Don't pay for a promise. Legitimate lenders never "guarantee" a card or loan before you apply. They may require that you pay application, appraisal, or credit report fees, but these fees seldom are required before the lender is identified and the application is completed. In addition, the fees generally are paid to the lender, not to the broker or person who arranged the "guaranteed" loan. Forward unsolicited email containing credit offers to spam@uce.gov.

8. Debt Relief

The Bait: Emails touting a way you can consolidate your bills into one monthly payment without borrowing; stop credit harassment, foreclosures, repossessions, tax levies and garnishments; or wipe out your debts.

The Catch: These offers often involve bankruptcy proceedings, but they rarely say so. While bankruptcy is one way to deal with serious financial problems, it's generally considered the option of last resort. The reason: it has a long-term negative impact on your creditworthiness. A bankruptcy stays on your credit report for 10 years, and can hurt your ability to get credit, a job, insurance, or even a place to live. To top it off, you will likely be responsible for attorneys' fees for bankruptcy proceedings.

Your Safety Net: Read between the lines when looking at these emails. Before resorting to bankruptcy, talk with your creditors about arranging a modified payment plan, contact a credit counseling service to help you develop a debt repayment plan, or carefully consider a second mortgage or home equity line of credit. One caution: While a home loan may allow you to consolidate your debt, it also requires your home as collateral. If you can't make the payments, you could lose your home.

Forward debt relief offers to spam@uce.gov.

9. Investment Schemes

The Bait: Emails touting "investments" that promise high rates of return with little or no risk. One version seeks investors to help form an offshore bank. Others are vague about the nature of the investment, but stress the rates of return. Promoters hype their high-level financial connections; the fact that they're privy to inside information; that they'll guarantee the investment; or that they'll buy it back. To close the deal, they often serve up phony statistics, misrepresent the significance of a current event, or stress the unique quality of their offering. And they'll almost always try to rush you into a decision.

The Catch: Many unsolicited schemes are a good investment for the promoters, but not for participants. Promoters of fraudulent investments operate a particular scam for a short time, close down before they can be detected, and quickly spend the money they take in. Often, they reopen under another name, selling another investment scam.

Your Safety Net: Take your time in evaluating the legitimacy of an offer: The higher the promised return, the higher the risk. Don't let a promoter pressure you into committing to an investment before you are certain it's legitimate. Hire your own attorney or an accountant to take a look at any investment offer, too.

Forward spam with investment-related schemes to spam@uce.gov.

10. Check Overpayment Scams

The Bait: A response to your ad or online auction posting, offering to pay with a cashier's, personal, or corporate check. At the last minute, the so-called buyer (or the buyer's "agent") comes up with a reason for writing the check for more than the purchase price, and asks you to wire back the difference after you deposit the check.

The Catch: If you deposit the check, you lose. Typically, the checks are counterfeit, but they're good enough to fool unsuspecting bank tellers and increase the balance in your bank account – temporarily. But when the check eventually bounces, you are liable for the entire amount.

Your Safety Net: Don't accept a check for more than your selling price, no matter how tempting the plea or convincing the story. Ask the buyer to write the check for the purchase price. If the buyer sends the incorrect amount, return the check. Don't send the merchandise. As a seller who accepts payment by check, you may ask for a check drawn on a local bank, or a bank with a local branch. That way, you can visit personally to make sure the check is valid. If that's not possible, call the bank the check was drawn on using the phone number from directory assistance or an internet site that you know and trust, not from the person who gave you the check. Ask if the check is valid.

Forward check overpayment scams to spam@uce.gov and your state Attorney General. You can find contact information for your state Attorney General at www.naag.org.

While you're online:

- Know who you're dealing with. In any electronic transaction, independently confirm the other party's name, street address, and telephone number.
- Resist the urge to enter foreign lotteries. These solicitations are phony and illegal.
- Delete requests that claim to be from foreign nationals asking you to help transfer their money through your bank account. They're fraudulent.
- Ignore unsolicited emails that request your money, credit card or account numbers, or other personal information.
- If you are selling something over the internet, don't accept a potential buyer's offer to send you a check for more than the purchase price, no matter how tempting the plea or convincing the story. End the transaction immediately if someone insists that you wire back funds.

The internet gives buyers access to a world of goods and services, and gives sellers access to a world of customers. Unfortunately, the internet also gives con artists the very same access. But being on guard online can help you maximize the global benefits of electronic commerce and minimize your chance of being defrauded.

Fighting Back

Con artists are clever and cunning, constantly hatching new variations on age-old scams. Still, skeptical consumers can spot questionable or unsavory promotions in email offers. Should you receive an email that you think may be fraudulent, forward it to the FTC at spam@uce.gov, hit delete, and smile. You'll be doing your part to help put a scam artist out of work.

Craigslist, Ebay and Other Online Scams

Scam's The Guru has personally dealt with

9-2-10 on craigslist I had an ad on craigslist trying to sell a laptop

jenifer cloud | jenifercloud@gmail.com

Re: HP Pavilion dv6258se Notebook PC - \$200 (Nashville)

1st email

Thanks for you reply,i am located in Remsenburg city in NY,i really need to buy this and send to my son schooling outside the state as a gift .I have been trying to buy this on ebay but its so very stressful buying on ebay.I will offer you \$230 so as to close the auction as soon as possible.I will be paying through PAYPAL because i have a verified account with paypal.So kindly get back with your paypal email address so i can make payment into your paypal account.Once payment clears,shipment will be handled by me through my personal fedex account,so you dont have to pay for shipment.Get back to me if my approval is granted.I would like to see the pictures please.

Thanks

3rd email

I have just made out the payment online now.Go and check the mail you used in opening your paypal account the confirmation mail have been sent there check the inbox or the spam message you should see it there..... I will also like you to know that i am having some little problems with my fedex account as i checked it online now and i was asked to reactivate it so i cant do that now as i have to sort one or two thing out with them.So i am sorry as i wont be handling shipment through my fedex account again.So, pls get the postage cost to the following address via post office(USPS EXPRESS MAIL INTERNATIONAL L at the usps office) and ship out the item via post office (EXPRESS MAIL) asap cos i have told my son to be expecting it. I have also included \$70 extra for the shipping. i think that should be enough for you to ship

NAME: Bamidele Tosin

Address: NO 4 madojutimi street

CITY: Abeokuta

STATE: Ogun state

COUNTRY: Nigeria

CODE:23439

Let me know how much it costs you to ship. After you ship get back to me with the amount you used to ship. .I am really sorry for the inconveniences.

Fake Paypal Confirmation Email

*****PROCEDURE FOR CREDITING ACCOUNT*****

charty212@gmail.com; on behalf of; service@paypal.com

pay.checkingcenter@accountant.com

Dear **paypalnashvilleguru@gmail.com**,

This is a confirmation email of the payment of \$300.00USD you received from Mrs Jenifer Cloud what is required of you in order for your account to be credited is the item's tracking/reference number, this number will be given to you at the courier office after you might have sent the item to the bearer, this is part of our new policy and a security measure in order to protect both the buyer and the seller, also to verify if the item was really bought from you we have sent you a confirmation email earlier to inform you that the payment is legal and has been confirmed, also to guide you against fraudulent acts.

We have included the buyer's full name and amount paid for you to know this message was really sent from PayPal. We advise that you make sure the item is sent out as soon as possible and request for a tracking number at the post office after you might have sent out the item, then you can email us the number by replying directly to this message after it might have been given to you at the courier office so as to credit your account without delay.

After we receive the number from you for security verification, your account will be credited at once, Our system has witness new upgrades, Please don't be surprised if you see us forwarding you to new customer attendants, its due to the amount of fraud going on involving our name which we are trying all our best to limit and put a stop to. As soon as we receive the requested information from you, your account will be credited.

PayPal Account Review Department.

Sincerely,

PayPal

Copyright © 2000-2010 PayPal. All rights reserved.

PayPal (Europe) Ltd. is [authorised and regulated by the Financial Services Authority](#) in the United Kingdom as an electronic money institution.

PayPal FSA Register Number: 226057

PayPal Email ID PP276

Things to Look For:

1. Someone contacted you from New York or anywhere else. (Why are they looking in the Nashville Craigslist)
2. They might have an American name when they contact you but want to it shipped to someone who has an obvious foreign name
3. How they contact you. A lot of emails will says. "I saw your advert" or "Is this item still for sale" and it's been like 2 minutes since the ad was up. An advert is an ad just a non-american word. Look at their Grammar and spelling, sometimes they are UK spelling.
4. Someone will be very interested in your item or service and offer you way more money then what you ask. I've been overnighed \$4,000, \$350, \$900 in checks. REAL people on craigslist are usually bargain hunters. No matter how low your price is they want you to go lower. So when you get someone who right from the start wants to offer more money then you are offering and then have it shipped BEWARE.
5. Paypal Email came from Europe, wait the person lives in New York or elsewhere. It contains my email address and not my full name. Email address that it came from is way to long and totally not from paypal. Claims that paypal will not credit my account until I ship item, that is not paypal policy.

A Real Paypal Email Received a Day Before Says

Payment received from Email address of sender
sendmail@paypal.com; on behalf of; Email address of sender

Hello Nashville Computer Guru,

You received a payment of \$24.99 USD from (Email Address of Sender).

To see all the transaction details, please log into your PayPal account. It may take a few moments for this transaction to appear in your account.

Most scams involve one or more of the following:

- Inquiry from someone far away, often in another country
- Western Union, Money Gram, cashier's check, money order, shipping, escrow service, or a "guarantee"
- Inability or refusal to meet face-to-face before consumating transaction

How To Avoid Craigslist Scams

You can sidestep would-be scammers by following these common-sense rules:

- DEAL LOCALLY WITH FOLKS YOU CAN MEET IN PERSON - follow this one simple rule and you will avoid 99% of the scam attempts on craigslist.

- NEVER WIRE FUNDS VIA WESTERN UNION, MONEYGRAM or any other wire service - anyone who asks you to do so is a scammer.
 - FAKE CASHIER CHECKS & MONEY ORDERS ARE COMMON, and BANKS WILL CASH THEM AND THEN HOLD YOU RESPONSIBLE when the fake is discovered later.
 - CRAIGSLIST IS NOT INVOLVED IN ANY TRANSACTION, and does not handle payments, guarantee transactions, provide escrow services, or offer "buyer protection" or "seller certification"
 - NEVER GIVE OUT FINANCIAL INFORMATION (bank account number, social security number, eBay/PayPal info, etc.)
 - AVOID DEALS INVOLVING SHIPPING OR ESCROW SERVICES and know that ONLY A SCAMMER WILL "GUARANTEE" YOUR TRANSACTION.
-

Examples of Scams

1. Someone claims that craigslist will guarantee a transaction, certify a buyer/seller, OR claims that craigslist will handle or provide protection for a payment.

These claims are fraudulent, as craigslist does not have any role in any transaction.

Scammer will often send an official looking email that appears to come from craigslist, offering a guarantee, certifying a seller, providing payment services -- all such emails are fakes!

2. Distant person offers a genuine-looking (but fake) cashier's check, you receive an email, offering to buy your item, or rent your apartment, sight unseen.

Cashier's check is offered for your sale item, as a deposit for an apartment, or for your services.

Value of cashier's check often far exceeds your item - scammer offers to "trust" you, and asks you to wire the balance via money transfer service

Banks will often cash these fake checks AND THEN HOLD YOU RESPONSIBLE WHEN THE CHECK FAILS TO CLEAR, including criminal prosecution in some cases!

Scam often involves a 3rd party (shipping agent, business associate owing buyer money, etc)

3. Someone requests wire service payment via Western Union or MoneyGram:

Scam "bait" items include apartments, laptops, TVs, cell phones, tickets, and other high value items

Often claim that an MTCN or confirmation code is needed before he can withdraw your money - this is FALSE, once you've wired money, it is GONE.

Common countries currently include: Nigeria, Romania, United Kingdom, Ukraine, Spain, Italy, Netherlands - but could be anywhere

Apartment listing may be local, but landlord/owner is "travelling" or "relocating" and needs you to wire money to them abroad , Deal often seems too good to be true, price is too low, rent is below market, etc

4. Distant person offers to send you a money order and then have you wire money:

This is ALWAYS a scam, in our experience - the cashier's check is FAKE, Sometimes accompanies an offer of merchandise, sometimes not , Scammer often asks for your name, address, etc for printing on the fake check , Deal often seems too good to be true

5. Distant seller suggests use of an online escrow service. Most online escrow sites are FRAUDULENT, operated by scammers, for more info, do a google search on "fake escrow" or "escrow fraud"

6. Distant seller asks for a partial payment upfront, after which he will ship goods, he says he trusts you with the partial payment , he may say he has already shipped the goods , deal often sounds too good to be true

7. Foreign company offers you a job receiving payments from customers, then wiring funds, Foreign company may claim it is unable to receive payments from its customers directly, You are typically offered a percentage of payments received , This kind of "position" may be posted as a job, or offered to you via email

Who should I notify about fraud or scam attempts?

FTC toll free hotline: 877-FTC-HELP (877-382-4357)

FTC online complaint form

Canadian PhoneBusters hotline: 888-495-8501

Competition Bureau Canada: 800-348-5358

Internet Fraud Complaint Center

Software Piracy (<http://www.siiia.net/piracy/report/>)

Non-emergency number for your local police department.

If you suspect that an item posted for sale on craigslist may be part of a scam, please email the details to "abuse@craigslist.org". Be sure to include the URL (or 10-digit post ID number) in your message.

Online Auctions Like Ebay

Internet auction sites give buyers a "virtual" flea market with new and used merchandise from around the world; they give sellers a global storefront from which to market their goods. But the online auction business can be risky business. Among the thousands of consumer fraud complaints the Federal Trade Commission (FTC) receives every year, those dealing with online auction fraud consistently rank near the top of the list. The complaints generally deal with late shipments, no shipments, or shipments of products that aren't the same quality as advertised; bogus online payment or escrow services; and fraudulent dealers who lure bidders from legitimate auction sites with seemingly better deals. Most complaints involve sellers, but in some cases, the buyers are the subject.

Thinking of bidding in an online auction, or selling some of your stuff? Internet auctions are a great resource for shoppers and sellers, but you need to watch out for some pitfalls. Here's how:

- **Evaluate how soon you need to receive the item you're bidding on, and whether you can tolerate it being delivered late, or even not delivered.** Many complaints about internet auction fraud involve late shipments, no shipments, or shipments of products that aren't the same quality as advertised.
 - **Whether you're a buyer or a seller, read each auction site's Terms of Use** before using it for the first time — sites may charge fees, follow different rules, or offer different protections.
 - **Carefully consider your method of payment.** Learn what recourse you have if something goes wrong. Don't send cash, and don't use a money wiring service. Credit Card is usual safe as your card company usually will refund your money and do a "charge back".
 - **Don't reply to "phishing" emails:** messages that look like they've been sent by an auction website or payment service and ask for your password or other personal information.
 - **Know who you're dealing with.** Avoid doing business with sellers you can't identify, especially those who try to lure you off the auction site with promises of a better deal. Confirm the seller's telephone number in case you have questions or problems.
 - **Know exactly what you're bidding on.** Read and print a copy of the seller's description of the product closely, especially the fine print. Save copies of all emails you send and receive from the auction site or seller, too.
-

7 Practices for Computer Security

Access to information and entertainment, credit and financial services, products from every corner of the world — even to your work — is greater than ever. Thanks to the internet, you can play a friendly game with an opponent across the ocean; review and rate videos, songs, or clothes; get expert advice in an instant; or collaborate with far-flung co-workers in a "virtual" office.

But the internet — and the anonymity it affords — also can give online scammers, hackers, and identity thieves access to your computer, personal information, finances, and more.

With awareness as your safety net, you can minimize the chance of an internet mishap. Being on guard online helps you protect your information, your computer, and your money. To be safer and more secure online, make these seven practices part of your online routine.

1. Protect your personal information. It's valuable.

To an identity thief, your personal information can provide instant access to your financial accounts, your credit record, and other assets. If you think no one would be interested in YOUR personal information, think again. ANYONE can be a victim of identity theft. In fact, according to the Federal Trade Commission, millions of people become victims every year. Visit [ftc.gov/idtheft](https://www.ftc.gov/idtheft) to learn what to do if your identity is stolen or your personal or financial information has been compromised — online or in the "real" world.

How do criminals get your personal information online? One way is by lying about who they are, to convince you to share your account numbers, passwords, and other information so they can get your money or buy things in your name. The scam is called "phishing": criminals send email, text, or pop-up messages that appear to come from your bank, a government agency, an online seller or another organization with which you do business. The message asks you to click to a website or call a phone number to update your account information or claim a prize or benefit. It might suggest something bad will happen if you don't respond quickly with your personal information. In reality, legitimate businesses should never use email, pop-ups, or text messages to ask for your personal information.

Some identity thieves have stolen personal information from many people at once, by hacking into large databases managed by businesses or government agencies. While you can't enjoy the benefits of the internet without sharing some personal information, you can take steps to share only with organizations you know and trust. Don't give out your personal information unless you first find out how it's going to be used and how it will be protected.

If you are shopping online, don't provide your personal or financial information through a company's website until you have checked for indicators that the site is secure, like a lock icon on the browser's status bar or a website URL that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some scammers have forged security icons. And some hackers have managed to breach sites that took appropriate security precautions.

Read website privacy policies. They should explain what personal information the website collects, how the information is used, and whether it is provided to third parties. The privacy policy also should tell you whether you have the right to see what information the website has about you and what security measures the company takes to protect your information. If you don't see a privacy policy — or if you can't understand it — consider doing business elsewhere.

2. Know who you're dealing with.

And what you're getting into. There are dishonest people in the bricks and mortar world and on the internet. But online, you can't judge an operator's trustworthiness with a gut-affirming look in the eye. It's remarkably simple for online scammers to impersonate a legitimate business, so you need to know who you're dealing with. If you're thinking about shopping on a site with which you're not familiar, do some independent research before you buy.

- If it's your first time on an unfamiliar site, call the seller's phone number, so you know you can reach them if you need to. If you can't find a working phone number, take your business elsewhere.
- Type the site's name into a search engine: If you find unfavorable reviews posted, you may be better off doing business with a different seller.
- Consider using a software toolbar that rates websites and warns you if a site has gotten unfavorable reports from experts and other internet users. Some reputable companies provide free tools that may alert you if a website is a known phishing site or is used to distribute spyware.

File-Sharing: Worth the hidden costs?

Every day, millions of computer users share files online. File-sharing can give people access to a wealth of information, including music, games, and software. How does it work? You download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. Often, the software is free and easy to access.

But file-sharing can have a number of risks. If you don't check the proper settings, you could allow access not only to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents. In addition, you may unwittingly download malware or pornography labeled as something else. Or you may download material that is protected by the copyright laws, which would mean you could be breaking the law.

If you decide to use file-sharing software, be sure to read the End User Licensing Agreement to be sure you understand and are willing to tolerate the potential risks of free downloads. As a computer technician, I can promise you that you will be infected shortly if you use P2P file sharing programs like LimeWire, Utorrent, Usenext, FrostWire and many others.

3. Use security software that updates automatically.

Keep your security software active and current: at a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. You can buy stand-alone programs for each element or a security suite that includes these programs from a variety of sources, including commercial vendors or from your Internet Service Provider. Security software that comes pre-installed on a computer generally works for a short time unless you pay a subscription fee to keep it in effect. In any case, security software protects against the newest threats only if it is up-to-date. That's why it is critical to set your security software to update automatically.

Some scam artists distribute malware disguised as anti-spyware software. Resist buying software in response to unexpected pop-up messages or emails, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers have used to spread malware. Once you confirm that your security software is up-to-date, run it to scan your computer for viruses and spyware. If the program identifies a file as a problem, delete it.

Anti-Virus Software

Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses, and then deleting them.

Anti-Spyware Software

Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your internet surfing, or record your keystrokes, which, in turn, could lead to the theft of your personal information.

A computer may be infected with spyware if it:

- Slows down, malfunctions, or displays repeated error messages
- Won't shut down or restart
- Serves up a lot of pop-up ads, or displays them when you're not surfing the web
- Displays web pages or programs you didn't intend to use, or sends emails you didn't write.
- Google searches are redirected to ads or other sites.

Firewalls

A firewall helps keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for outside attempts to access your system and blocking communications to and from sources you don't permit.

Don't Let Your Computer Become Part of a "BotNet"

Some spammers search the internet for unprotected computers they can control and use anonymously to send spam, turning them into a robot network, known as a "botnet." Also known as a "zombie army," a botnet is made up of many thousands of home computers sending emails by the millions. Most spam is sent remotely this way; millions of home computers are part of botnets.

Spammers scan the internet to find computers that aren't protected by security software, and then install bad software – known as "malware" – through those "open doors." That's one reason why up-to-date security software is critical.

Malware may be hidden in free software applications. It can be appealing to download free software like games, file-sharing programs, customized toolbars, and the like. But sometimes just visiting a website or downloading files may cause a "drive-by download," which could turn your computer into a "bot."

Another way spammers take over your computer is by sending you an email with attachments, links or images which, if you click on or open them, install hidden software. Be cautious about opening any attachments or downloading files from emails you receive. Don't open an email attachment — even if it looks like it's from a friend or coworker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is.

4. Keep your operating system and Web browser up-to-date, and learn about their security features.

Hackers also take advantage of Web browsers (like Firefox or Internet Explorer) and operating system software (like Windows or Mac's OS) that don't have the latest security updates.

In addition, you can increase your online security by changing the built-in security and privacy settings in your operating system or browser. Check the "Tools" or "Options" menus to learn how to upgrade from the default settings. Use your "Help" function for more information about your choices.

If you're not using your computer for an extended period, disconnect it from the internet. When it's disconnected, the computer doesn't send or receive information from the internet and isn't vulnerable to hackers.

Also if you have wireless internet, you can encrypt the SSID (Wireless Network Name) to prevent other people from getting on your network and even your computer. Additionally you can change the router user name and password and prevent it from broadcasting the SSID which means people won't even know your wireless exist.

5. Protect your passwords.

Keep your passwords in a secure place, and out of plain sight. Don't share them on the internet, over email, or on the phone. Your Internet Service Provider (ISP) should never ask for your password.

In addition, hackers may try to figure out your passwords to gain access to your computer. To make it tougher for them:

- Use passwords that have at least eight characters and include numbers or symbols. The longer the password, the tougher it is to crack. A 12-character password is stronger than one with eight characters.
- Avoid common words: some hackers use programs that can try every word in the dictionary.
- Don't use your personal information, your login name, or adjacent keys on the keyboard as passwords.
- Change your passwords regularly (at a minimum, every 90 days).
- Don't use the same password for each online account you access.

6. Back up important files.

If you follow these tips, you're more likely to be free of interference from hackers, viruses, and spammers. But no system is completely secure. If you have important files stored on your computer, copy them onto a removable disc or an external hard drive, and store it in a safe place.

7. Learn what to do in an e-emergency.

If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information. Malware could be sending your personal information to identity thieves.

Confirm that your security software is up-to-date, then use it to scan your computer. Delete everything the program identifies as a problem. You may have to restart your computer for the changes to take effect.

If the problem persists after you exhaust your ability to diagnose and treat it, you might want to call for professional help. If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem. Your notes will help you give an accurate description to the technician.

If you need professional help, if your machine isn't covered by a warranty, or if your security software isn't doing the job properly, you may need to pay for technical support. Many companies — including some affiliated with retail stores — offer tech support via the phone, online, at their store, or in your home. Telephone or online help generally are the least expensive ways to access support services — especially if there's a toll-free helpline — but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a technician or repair person to come into your home.

Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do to avoid it in the future.

Also, talk about safe computing with anyone else who uses the computer. Tell them that some online activity can put a computer at risk, and share the seven practices for safer computing.

Tips for Parents

Parents sometimes can feel outpaced by their technologically savvy kids. Technology aside, there are lessons that parents can teach to help kids stay safer as they socialize online. Most ISPs provide parental controls, or you can buy separate software. But no software can substitute for parental supervision. Talk to your kids about safe computing practices, as well as the things they're seeing and doing online.

Identity Theft

It's important to protect your personal information, and to take certain steps quickly to minimize the potential damage from identity theft if your information is accidentally disclosed or deliberately stolen:

- Place a "Fraud Alert" on your credit reports, and review those reports carefully. Notifying one of the three nationwide consumer reporting companies is sufficient.
- Close any accounts that have been tampered with or established fraudulently.
- File a police report with local law enforcement officials. This is an essential step in claiming your rights.
- Report your theft to the Federal Trade Commission, [online](#), by phone, or by mail.

And before identity theft happens, learn how to safeguard your information at [ftc.gov/idtheft](https://www.ftc.gov/idtheft).

Social Networking Sites

While social networking sites can increase a person's circle of friends, they also can increase exposure to people with less than friendly intentions.

Here are tips for helping your kids and you to use social networking sites safely:

- Help your kids understand what information should be private.
- Explain that kids should post only information that you – and they – are comfortable with others seeing.
- Use privacy settings to restrict who can access and post on your child's website.
- Remind your kids that once they post information online, they can't take it back.
- Talk to your kids about avoiding sex talk online.
- Tell your kids to trust their gut if they have suspicions. If they ever feel uncomfortable or threatened by anything online, encourage them to tell you.
- When getting emails, Facebook or MySpace messages from friends but they have strange links inside such as <http://www.opjfpjpwejfjdd.net/2jowjfoij> or <http://208.342.32.12/systemscan> beware, most likely your friend didn't send those but instead they are infected and the program on their computer sent out these messages to you in hopes you will trust the source. Be careful when clicking links as sometimes they are phishing. It can say <http://www.paypal.com> but when you place your mouse over it, it shows <http://292.423.12.121/paypal/> this is without a doubt a phishing scam so delete that message.

Social Networking Sites: A Parent's Guide

"It's 10 p.m. Do you know where your children are?"

Remember that phrase from your own childhood? It's still a valid question, but now, it comes with a twist: "Do you know where your kids are — and who they're chatting with online?"

Social networking sites have morphed into a mainstream medium for teens and adults. These sites encourage and enable people to exchange information about themselves, share pictures and videos, and use blogs and private messaging to communicate with friends, others who share interests, and sometimes even the world-at-large. And that's why it's important to be aware of the possible pitfalls that come with networking online.

Some social networking sites attract pre-teens – even kids as young as 5 or 6. These younger-focused sites don't allow the same kinds of communication that teens and adults have, but there are still things that parents can do to help young kids socialize safely online. In fact, when it comes to young kids, the law provides some protections – and gives parents some control over the type of information that children can disclose online. For sites directed to children under age 13, and for general audience sites that know they're dealing with kids younger than 13, there's the Children's Online Privacy Protection Act (COPPA). It requires these sites to get parental consent before they collect, maintain, or use kids' information. COPPA also allows parents to review their child's online profiles and blog pages.

Parents sometimes can feel outpaced by their technologically savvy kids. Technology aside, there are lessons that parents can teach to help kids stay safer as they socialize online.

Help Kids Socialize Safely Online

Here are some tips for safe social networking:

- **Help your kids understand what information should be private.** Tell them why it's important to keep some things – about themselves, family members and friends – to themselves. Information like their full name, Social Security number, street address, phone number, and family financial information — like bank or credit card account numbers — is private and should stay that way. Tell them not to choose a screen name that gives away too much personal information.
- **Use privacy settings to restrict who can access and post on your child's website.** Some social networking sites have strong privacy settings. Show your child how to use these settings to limit who can view their online profile, and explain to them why this is important.
- **Explain that kids should post only information that you — and they — are comfortable with others seeing.** Even if privacy settings are turned on, some — or even all — of your child's profile may be seen by a broader audience than you're comfortable with. Encourage your child to think about the language used in a blog, and to think before posting pictures and videos. Employers, college admissions officers, team coaches, and teachers may view your child's postings. Even a kid's screen name could make a difference. Encourage teens to think about the impression that screen names could make.
- **Remind your kids that once they post information online, they can't take it back.** Even if they delete the information from a site, older versions may exist on other people's computers and be circulated online.
- **Know how your kids are getting online.** More and more, kids are accessing the internet through their cell phones. Find out about what limits you can place on your child's cell phone. Some cellular companies have plans that limit downloads, internet access, and texting; other plans allow kids to use those features only at certain times of day.
- **Talk to your kids about bullying.** Online bullying can take many forms, from spreading rumors online and posting or forwarding private messages without the sender's OK, to sending threatening messages. Tell your kids that the words they type and the images they post can have real-world consequences. They can make the target of the bullying feel bad, make the sender look bad – and, sometimes, can bring on punishment from the authorities. Encourage your kids to talk to you if they feel targeted by a bully.
- **Talk to your kids about avoiding sex talk online.** Recent research shows that teens who don't talk about sex with strangers online are less likely to come in contact with a predator.

If you're concerned that your child is engaging in risky online behavior, you can search the blog sites they visit to see what information they're posting. Try searching by their name, nickname, school, hobbies, grade, or area where you live.

- **Tell your kids to trust their gut if they have suspicions.** If they feel threatened by someone or uncomfortable because of something online, encourage them to tell you. You can then help them report concerns to the police and to the social networking site. Most sites have links where users can immediately report abusive, suspicious, or inappropriate online behavior.
- **Read sites' privacy policies.** Spend some time with a site's privacy policy, FAQs, and parent sections to understand its features and privacy controls. The site should spell out your rights as a parent to review and delete your child's profile if your child is younger than 13.

A Few More Tips to Protect Pre-Teens

Many of the tips above apply for pre-teens, but parents of younger children also can:

- **Take extra steps to protect younger kids.** Keep the computer in an open area like the kitchen or family room, so you can keep an eye on what your kids are doing online. Use the internet with them to help develop safe surfing habits. Consider taking advantage of parental control features on some operating systems that let you manage your kids' computer use, including what sites they can visit, whether they can download items, or what time of day they can be online.
- **Go where your kids go online.** Sign up for – and use – the social networking spaces that your kids visit. Let them know that you're there, and help teach them how to act as they socialize online.

- **Review your child's friends list.** You may want to limit your child's online “friends” to people your child actually knows and is friendly with in real life.
- **Understand sites' privacy policies.** Sites should spell out your rights as a parent to review and delete your child's profile if your child is younger than 13.

For More Information

Federal Trade Commission — www.OnGuardOnline.gov

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.

The FTC manages OnGuardOnline.gov, which provides practical tips from the federal government and the technology industry to help you be on guard against internet fraud, secure your computer, and protect your personal information.

ConnectSafely — www.connectsafely.org

ConnectSafely.org is the leading interactive resource on the Web for parents, teens, educators – everyone interested in youth safety on the fixed and mobile social Web. In addition to the discussion forum, it provides tips, news, and other resources for safe, constructive use of digital media and technologies. Along with NetFamilyNews.org, ConnectSafely is a project of the non-profit Tech Parenting Group.

Cyberbully411 — www.cyberbully411.org

Cyberbully411 provides resources and opportunities for discussion and sharing for youth - and their parents - who have questions about or may have been targeted by online harassment. The website was created by the non-profit Internet Solutions for Kids, Inc., with funding from the Community Technology Foundation of California.

GetNetWise — www.getnetwise.org

GetNetWise is a public service sponsored by internet industry corporations and public interest organizations to help ensure that internet users have safe, constructive, and educational or entertaining online experiences. The GetNetWise coalition works to provide internet users with the resources they need to make informed decisions about their and their family's use of the internet.

Internet Keep Safe Coalition — www.iKeepSafe.org

iKeepSafe.org is a coalition of 49 governors/first spouses, law enforcement, the American Medical Association, the American Academy of Pediatrics, and other associations dedicated to helping parents, educators, and caregivers by providing tools and guidelines to promote safe internet and technology use among children.

National Center for Missing and Exploited Children — www.missingkids.com; www.netsmartz.org

The NetSmartz Workshop is an educational safety resource from the National Center for Missing & Exploited Children that uses age-appropriate, interactive activities to teach children of all ages how to stay safer on the internet.

staysafe — www.staysafe.org

staysafe.org is an educational site intended to help consumers understand both the positive aspects of the internet as well as how to manage a variety of safety and security issues that exist online.

Wired Safety — www.wiredsafety.org

WiredSafety.org is an internet safety and help group. WiredSafety.org provides education, assistance, and awareness on cybercrime and abuse, privacy, security, and responsible technology use. It is also the parent group of Teenangels.org, FBI-trained teens and preteens who promote internet safety.

See also:

[Social Networking Sites: Safety Tips for Tweens and Teens](#)

What to Do if There's a Problem

Trust your gut if you have suspicions. If you feel threatened by someone or uncomfortable because of something online, tell an adult you trust, and report it to the police and the social networking site.

The Children's Online Privacy Protection Act (COPPA) requires websites to obtain parental consent before collecting, using, or disclosing personal information from children under age 13. If a website is violating COPPA, report it to the [Federal Trade Commission](#).

For More Information and Who To Report Too:

Identity Theft: What To Do If Your Personal Information Has Been Compromised

The bottom line for online threats like phishing, spyware, and hackers is identity theft. ID theft occurs when someone uses your name, Social Security number, credit card number or other personal information without your permission to commit fraud or other crimes. That's why it's important to protect your personal information. To find out how to deter and detect identity theft, visit ftc.gov/idtheft.

But, according to OnGuard Online, if your personal information is accidentally disclosed or deliberately stolen, taking certain steps quickly can minimize the potential for the theft of your identity.

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:
 - TransUnion: www.transunion.com, 1-800-680-7289
 - Experian: www.experian.com, 1-888-EXPERIAN (397-3742)
 - Equifax: www.equifax.com, 1-800-525-6285

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

- **Close accounts.** Close any accounts that have been tampered with or established fraudulently:

- Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
- Use the [ID Theft Affidavit](#) to support your written statement.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime. This report will also help you claim your rights as a victim of identity theft.
- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.

Online: www.ftc.gov/complaint

By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

Alert the appropriate authorities by contacting:

- Your ISP and the hacker's ISP (if you can tell what it is). You can usually find an ISP's email address on its website. Include information on the incident from your firewall's log file. By alerting the ISP to the problem on its system, you can help it prevent similar problems in the future.
- The FBI at www.ic3.gov. To fight computer criminals, they need to hear from you.

How to Report Internet Fraud

If a scammer takes advantage of you through an internet auction, when you're shopping online, or in any other way, report it to the Federal Trade Commission, at www.ftc.gov/complaint. The FTC enters internet, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

How to Report Deceptive Spam

- If you get deceptive spam, including email phishing for your information, forward it to spam@uce.gov. Be sure to include the full header of the email, including all routing information.
- You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.

Divulged Personal Information

If you believe you have mistakenly given your personal information to a fraudster, file a complaint at www.ftc.gov/complaint, and then visit the Federal Trade Commission's Identity Theft website at ftc.gov/idtheft to learn how to minimize your risk of damage from a potential theft of your identity.

Social Networking Sites

Trust your instincts – and tell kids to trust theirs - if you (or they) are suspicious about something on a social networking site. If kids feel threatened by someone or uncomfortable because of something online, encourage them to tell you. You can then help them report concerns to the police and to the social networking site. Most sites have links where users can immediately report abusive, suspicious, or inappropriate online behavior.

How to Report a Cross-Border Scam

If you think you may have responded to a **cross-border scam**:

- File a complaint at www.econsumer.gov, a project of 20 countries of the [International Consumer Protection and Enforcement Network](#).
- Then visit the FTC's identity theft website at ftc.gov/idtheft. While you can't completely control whether you will become a victim of identity theft, you can take some steps to minimize your risk.

If you've responded to a "**Nigerian**" or other **advance fee schemes**:

- Contact your local Secret Service field office using contact information from the Blue Pages of your telephone directory, or from www.secretservice.gov/field_offices.shtml.

If you've experienced **telemarketing fraud** or **check overpayment scams**:

- Report it to your state Attorney General, using contact information at naag.org.

If you get **unsolicited email offers**, or **spam** – including offers inviting you to participate in a foreign lottery, looking for help getting money out of a foreign country, or asking you to wire back extra funds from a check you received:

- Send the messages to spam@uce.gov.

If you get what looks like **lottery material** from a foreign country through the postal mail:

- Give it to your local postmaster.

Foreign Lottery Scams

[U.S. Federal Trade Commission](#) — The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

[Competition Bureau in Canada](#) — The Competition Bureau is an independent law enforcement agency in Canada that investigates anti-competitive practices and promotes compliance with the laws under its jurisdiction. To file a complaint or to get free information, visit www.competitionbureau.gc.ca or call toll-free, 1-800-348-5358. The Bureau has the ability to refer criminal matters to the Attorney General of Canada, who then decides whether to prosecute before the courts.

[United Kingdom's Office of Fair Trading](#) — The United Kingdom's Office of Fair Trading is responsible for making markets work well for consumers. They protect and promote consumer interests throughout the United Kingdom, while ensuring that businesses are fair and competitive. To file a complaint or to get free information, visit www.oft.gov.uk or send an email to enquiries@oft.gsi.gov.uk.

[Australian Competition and Consumer Commission](#) — The Australian Competition and Consumer Commission encourages vigorous competition in the marketplace and enforces consumer protection and fair trading laws. To file a complaint or to get more information, visit www.accc.gov.au. The ACCC advocates consultation and

negotiation as the first and best option to settle disputes, but once the ACCC pursues legal action any sort of mediation becomes less likely.

"Nigerian" and other Advance-Fee Scams

[U.S. Secret Service](#) — The Secret Service investigates violations of laws relating to financial crimes, including access device fraud, financial institution fraud, identity theft, and computer fraud. To file a complaint or to get free information, visit www.secretservice.gov or call 202-406-5708.

[U.S. Department of State](#) — The Department of State's mission is to create a more secure, democratic, and prosperous world for the benefit of the American people and the international community. As part of that mission, the Department of State seeks to minimize the impact of international crime, including cross-border internet scams, on the United States and its citizens. To get free information, visit www.state.gov.

[U.S. Federal Trade Commission](#) — See above.

How to Report Problems with Online Auctions

If you have problems during a transaction, try to work them out directly with the seller, buyer, or site operator. If that doesn't work, file a complaint with:

- the Federal Trade Commission at www.ftc.gov/complaint.
- your state Attorney General, using contact information at naag.org.
- your county or state consumer protection agency. Check the blue pages of the phone book under county and state government, or visit consumeraction.gov and look under "Where to File a Complaint."
- the [Better Business Bureau](#).

Tips for the Offline World that you can do Online:

For the offline world, sometimes you may want to find out more information about someone like if they have a criminal record

For Nashville you can view their Criminal Clerk Website to do free searches.

<http://ccc.nashville.gov/portal/page/portal/ccc/caseSearch/caseSearchPublic/caseSearchPublicForms>

For internet wide you can search either by name, ie, a tech coming to your house or anything other person who is coming to your place and want to see if there is any known background you can use this website. You can also search businesses too.

<http://pipl.com/>