



# How to Protect Yourself Online

## ....by reducing spam

**What is Spam?** Years ago “spam” was canned meat you purchased at the grocery store. Today “spam” has another meaning. Spam is junk email. Most spam is annoying, time-consuming, and costly. But sometimes spam is used to cause harm, created specifically to steal your personal information or to damage your computer.

Types  
of  
harmful  
spam:

**Spyware** steals your personal information

**Malware** makes your computer sick by implanting viruses

## Ways to reduce spam and keep your computer healthy:

- ✓ Choose an email provider with a strong spam blocker.
- ✓ If your email service provides it, use the “This is spam” button. This tells your provider what emails you don’t want to receive.
- ✓ If you do not recognize a sender’s name, do not open it – the email is probably spam.
- ✓ Never respond to spam even if your intent is to be removed from the spammer’s mailing list.
- ✓ Do not post your email address on a public forum or website.
- ✓ Only share your email address with people or groups you know.
- ✓ Even if you know the sender, be cautious about opening attachments or downloading files.
- ✓ Set your Inbox so that emails do not automatically display logos and pictures or download attachments.
- ✓ Install anti-spyware and anti-virus software. Sometimes this software is already pre-installed on your new device. If it isn’t, you can download it from your Internet Service Provider or purchase it in retail stores.
- ✓ Download free software only from sites you know and believe are genuine.
- ✓ Turn on your firewall (a software program or piece of hardware) that helps screen and block harmful communications.

## Signs and symptoms your computer may have a virus:

- Your computer is displaying **a lot** of pop-up messages – especially ads for buying and installing anti-virus software.
- Your computer has gone rogue and is sending out email messages to all of your contacts.
- Your computer runs unusually slow.
- Your computer frequently freezes or crashes.
- Your files, folders or icons vanish.
- Your anti-virus software disappears.
- Your computer won't let you update your anti-virus software.
- Your computer has new programs that you didn't install.

## What to do if your computer is infected:

- Immediately stop using your computer for any activity, like banking or shopping, that involves sensitive information such as passwords, credit card or social security numbers.
- Run your anti-virus software (assuming it wasn't deleted!). After the virus has been removed, shut down your computer and reboot. Now run the anti-virus software a second time just to be sure.
- If your computer is under a warranty that includes free tech support, you may wish to take advantage of this service.
- If you don't have a warranty but feel like you're in over your head, many companies and some retail stores offer over-the-phone, in-store or in-home tech support.
- Once your computer has a clean bill of health, follow the tips on the reverse side to keep it happy, healthy and virus-free!

### For additional information:

<http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email>

<http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business>

<http://www.onguardonline.gov/articles/0038-spam/>





# How to Protect Yourself Online

## ....by avoiding scams

**Don't Fall for that Scam!** Email is a fun, fast and convenient way to communicate with friends and family. But unfortunately email can also be an easy and convenient way for crooks and scammers to defraud millions of people each year. Many scammers create emails impersonating a business (like your bank or credit card company) or a government agency and then try to trick you into providing your personal information. This is call “phishing.” Below are some ways you can avoid phishing scams:

### Ways you can avoid being scammed:

- ✓ Never provide your personal or financial information, social security number, user names or passwords in response to an email. A legitimate company will **never** ask you to provide confidential information in an email.

*Examples of a phishing email:*

*“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 could not verify your information. Please click here to update and verify your information.”*

- ✓ Never reply to phishing emails. Do not click on any links or call any phone numbers provided in the email.
- ✓ If you are unsure whether an email is really from a legitimate business you know, contact the business using a telephone number – a telephone number that you have in your records, not the one provided in the questionable email.
- ✓ Review account and credit card statements promptly to check for unauthorized charges. If you notice any questionable charges, call the number on your statement to ask about the charges.
- ✓ Forward suspected phishing emails to the company being imitated and also to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov)

