Staying Safe Online

Keeping your information safe while using email, visiting websites, and buying online.

What you put on the Internet may be stored there, and available there, for a long, long time. Information that is published on a web page, comments that you type into a website, information that you enter into a form on a web page, can be available for years and years.

See archival content from the web at http://www.archive.org

Some people have suggested that if you wouldn't want it published in a newspaper then you shouldn't put it on the web, particularly things that may be embarrassing for you later on.

Your email address may end up somewhere unanticipated if you respond to a spam email to "unsubscribe" or "opt-out", if you enter a contest online, or if you or someone else puts your email address into a form on a website.

It's possible that someone who has your email address may try to log into financial or store sites online using it.

When you enter personal information on the web, read the Privacy Statement first - you might be surprised to learn exactly what they say they may do with the information they collect from you.

It's important not to use your own personal information in a password, and don't use the same password across multiple websites. Don't use passwords that can be guessed at if someone knows about you, where you live, your house number, or your pet's name.

Strong passwords use a combination of upper and lowercase letters, numbers, and punctuation. Use the first letters of a phrase, line of poetry, or song lyric that is familiar to you for your password.

Check your password at http://www.microsoft.com/protect/yourself/password/checker.mspx

Protect your email address. If you need to use a temporary or secondary email address, sign up for a free Yahoo or Gmail email address. That way you can cancel it if you need to (but read their privacy policy too!)

If you want to register for something online, see if you can give them just the minimal amount of information they require rather than everything that they request.

PHISHING is when you are tricked into thinking a website or email is something it is not. Be careful about phishing emails that could be directing you to a fake website. Be wary of emails that are not addressed directly to you and which have links embedded in them.

Phishing tip-offs are bad grammar, missing images, URL addresses that don't match the site address, urgent requests for login information or even social security numbers and PIN numbers.

Even if you get an email that you think is from a company that you know and trust, rather than clicking on a link in the email, type the web address into your web browser yourself. That way you know that you are going to the correct site.

Don't guess at web addresses if you are going to be dealing with personal information. Find the exact URL on your credit card or bank statement.

Be careful about entering financial information into public computers. Spyware may be running in the background. Ask about the security precautions the library or internet café takes.

Before entering any financial or secure personal information, make sure that the web page is a secure page by looking for the lock or key icon on your browser window.

Protect your computer with anti-virus and anti-spyware software if it is vulnerable, and keep it up-to-date with weekly updates.

Author of this work: Bob Raiselis