How to Protect Yourself Online

FCC
Consumer Facts

Background

The Internet and the information it connects to is a resource that many have come to depend upon. Facts that once might have taken several days to locate in a research library can now be obtained instantaneously using your personal computer or even a handheld wireless device. Individuals can publish to a world wide audience, mix up previously existing content to form new creations, or act as curators, sharing with friends the best new content found on the Internet. Because almost anyone with a computer or wireless device can connect to the Internet, however, some bad actors have found ways to use it to cause harm. Several US Government agencies, including the Federal Communications Commission (FCC), and non-profit organizations have joined in an effort to provide consumers useful, easy-to-understand information on Internet safety that can be found at www.onguardonline.gov. This guide summarizes some of this valuable information.

Spam (and What it Can Lead To)

"Spam" is online junk mail, which is inconvenient and wastes time. Spam can change from annoying to malicious if spam emails, or anything attached to them, steal personal information (spyware) or work to disrupt your personal computer or wireless device by implanting viruses or worms (malware). Some malware can integrate your computer into a network to distribute spam, turning it into a "zombie" that becomes part of a "botnet." Ways you can reduce spam include:

- Look for an email provider with strong anti-spam filtering capability. You don't have to use the email service provided by your Internet Service Provider (ISP), the company from which you purchase your access to the Internet, but can chose an independent email service. One way email providers compete for your business is to provide better filtering capability. You can also talk to your provider if you think spam filtering could be improved.

- Some email spam filters have settings that can be changed to make them stronger. Check your filter to be sure it's set where you want it to be. If you have questions about changing settings, contact your email provider.

Spam (and What it Can Lead To) (cont'd.)

- Identify unwanted spam with the "spam" button. Many email services allow you to select spam email, and then push a "spam" button to identify it as unwanted email. Use this button if you have it, because it lets your email provider know what email you don't want.

- Email settings also allow you to prevent images such as logos and pictures from automatically displaying when you open an incoming email. Open images can contain malware and spyware and let spammers know their emails have been opened, and thus that the emails have been sent to a valid address.

- Set your email so that it doesn't automatically accept incoming appointments or automatically download attachments, again so that you don't let spammers know the email has been sent to a valid address.

- Try to limit sending or displaying your email address to people or groups you know. Check the privacy policy before sending your address to a Web site or directory, and, if you can, "opt out" of allowing your address to be shared.

- Protect your friends' addresses by putting them on the "bcc" line when sending emails to a group of people who don't know each other.

(More) →

Spam (and What it Can Lead To) (cont'd.)

- Consider using two email addresses, one for personal mail, and one for correspondence with companies or groups that you deal with regularly.

- Never respond to spam.

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, a federal law, requires senders of commercial email to give you a return email address or other Internet-based response method to opt out of future emails. Senders must honor your opt out request within ten days, and cannot sell or transfer the email address in your opt out request unless the transfer is to allow another sender to comply with the Act. Find out more about the Act at **www.ftc.gov/spam**. You can report spam received on your computer to the Federal Trade Commission (FTC) by sending a copy of the message to **spam@uce.gov**. The CAN-SPAM Act also prohibits the sending of unwanted commercial messages to wireless devices using an Internet address without prior authorization. For more information on spam to wireless devices and how to complain to the FCC about it, see the FCC consumer guide at **www.fcc.gov/guides/spam-unwanted-text-messages-and-email**.

Ways you can control spyware and malware that may come with spam are:

- Install anti-virus and anti-spyware software, which scans incoming emails and files for problems, and keep it up to date. This software may come pre-installed on a new computer or device, can be downloaded from your ISP or software company websites, or purchased in retail stores. Because bad actors continually come up with new viruses and spyware, your software needs to be updated regularly. Some software updates automatically.

- Set your operating system software (such as Windows or an Apple computer operating system) to automatically download and install new security patches.

Spam (and What it Can Lead To) (cont'd.)

- Be careful about opening attachments or downloading files, even if you think you know the sender. The cover email should mention the attachment and describe what's in it.

- Download free software, including games and toolbars, only from sites you know and believe are genuine.

- Use a firewall, which blocks all incoming communications from unauthorized sources, when connected to the Internet.

Signs that your computer may be infected include slowing, repeated error messages, increasing numbers of pop-up ads, or going to websites other than the one you intend. Scan your computer regularly, and contact your security software provider or seek other professional help if you find problems you can't solve. You can also complain about an infection to the FTC online at **https://www.ftccomplaintassistant.gov**, calling toll-free to 1-877-382-4357 (voice) or 1-866-653-4261 (TTY), or writing to:

Federal Trade Commission
CRC-240
600 Pennsylvania Ave., NW,
Washington, DC 20580.

Scams

Some of the most dangerous spam emails are those that are disguised as legitimate emails from a business or organization that you may do business with, such as your bank, credit card company, club you belong to, or even a government agency. The emails ask that you update or confirm account or other personal information, and provide a link to a Web site that looks just like the website of the "organization" contacting you. In a new twist, such "phishing" scams are being used to obtain user names and passwords to email accounts, allowing scammers access to all the personal information contained in your own emails and any emails sent to you by

(More)

Scams (cont'd.)

others. Phishing scams can also lead to identity theft. Here are ways to avoid these scams:

- Don't provide personal or financial information, user names, or passwords in response to an email, because legitimate companies generally don't seek such information in this way.
- If you question whether an email is really from a legitimate business you know, contact the business using a phone number or web address other than the one provided in the email, and ask if the business sent it.
- Use the security tips for preventing spam and spyware or malware listed above.
- Review account and credit card statements promptly to check for unauthorized charges. Use the number or web address on the statement to contact the statement sender if you see any such charges.
- Forward suspected phishing emails to the organization that is being imitated and to the FTC at **spam@uce.gov**. If you think you've been the victim of phishing or another scam, report it to the FTC using the contact information provided above. You can also visit the FTC's Identity Theft website at **www.ftc.gov/bcp/edu/microsites/idtheft/** to find ways to prevent this additional problem.

In addition to phishing emails, watch out for emails with sales pitches or promises that sound too good to be true. Before buying or otherwise acting on an online offer, get all your questions answered and read all the fine print. For more information on common email scams, go to **www.ftc.gov/bcp/menus/consumer/tech/scams.shtm**.

Got Kids?

Any parent or caregiver knows that children are spending more time online and at younger ages. With newer and increasingly popular smart phones, Internet access is easier than ever. Children can be more vulnerable to scams and sophisticated online marketing, and are sharing more personal information on social networking sites. The best advice for parents and caregivers is to talk to children about Internet safety and stay aware of what children are doing online. For more information on children's Internet safety, go to **www.onguardonline.gov/topics/net-cetera.aspx**.

For More Information

For information about other communications issues, visit the FCC's Consumer & Governmental Affairs Bureau website at **http://www.fcc.gov/consumer-governmental-affairs-bureau**, or contact the FCC's Consumer Center by calling 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY; faxing 1-8666-418-0232; or writing to:

Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, D.C. 20554.

###

For this or any other consumer publication in an accessible format (electronic ASCII text, Braille, large print, or audio), please write or call us at the address or phone number below, or send an email to ***FCC504@fcc.gov*** *.*

To receive information on this and other FCC consumer topics through the Commission's electronic subscriber service, visit ***www.fcc.gov/cgb/contacts/****.*

This document is for consumer education purposes only and is not intended to affect any proceedings or cases involving this subject matter or related issues.