What You Can Do About Junk Email

From the Office of Minnesota Attorney General Keith Ellison

By some estimates, spammers send up to one billion junk emails a day. Although most are never opened, enough people click on the links to make junk email, also called "spam," a lucrative industry. Spam emails not only are a nuisance but also can damage your computer and allow an attacker access to your private and financial information.

Junk emails take many forms. Some are attempts to sell questionable products, such as herbal supplements or weight loss services. Others are attempts to commit financial fraud, such as "phishing" schemes designed to dupe citizens into giving out their private banking information to a scam artist, or so called "Nigerian investment scams," in which the sender poses as a foreign bank official to lure citizens into supplying account information to a criminal.

So what can a consumer do? The following tips are designed to protect your computer and you from becoming a victim of fraud or damage perpetrated through junk emails.

Disguised and Dangerous

"Phishing"

Some scammers pose as legitimate banks, retailers, employers, or social networking "friends" in order to get people to inadvertently supply personal information, such as banking details and passwords. The scammers then use the personal information to drain bank accounts or steal the citizen's identity. Remember: reputable organizations do not ask you to respond to emails by supplying personal information.

"Spear Phishing"

"Spear phishing" involves a scammer sending personalized messages to an organization from what appears to be a trusted source, such as an IT staff member asking for personal information or passwords. Spear phishing attacks have occurred at financial institutions, law firms, and government offices.

Spyware and Malware

A lot of spam is sent out by networks of "zombie" computers or "bots" that have been infected by spyware and are used by criminals. Law-abiding citizens may not even know their computers are unwittingly sending spam.

The Federal CAN-SPAM Act

A federal law, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, or the "CAN-SPAM Act," has been ineffective in curbing the growing deluge of junk email. The CAN-SPAM Act only requires senders of junk email to follow certain nominal rules. For example, senders may not use other companies' domain names, email subject headers must not be deceptive, and sexually explicit email must be labeled as such. Spam email must also offer a way for the citizen to "opt out" of receiving future emails, and the sender has ten business days to comply.

The CAN-SPAM Act is enforced by the Federal Trade Commission (FTC). If you have a complaint about junk emails, you should contact the FTC's toll-free helpline: (877) FTC-HELP ((877) 382-4357).

Dealing With Unwanted Emails

The following are some tips to deal with unwanted emails:

1. **Most operating systems can have multiple user accounts with different privileges.** An easy and cheap way to help protect against attack is to set up a "user" account on your computer that, unlike the "administrator" account, does not have the right to install software. If you read email and browse the internet with the user account, some malicious software will be unable to secretly install itself without your permission.

2. **Install security software.** Make sure that you purchase security software from a business or individual you know and trust. Do not purchase security software in response to a phone message or computer pop-up telling you your computer has a virus or has been hacked—this is another scam. For more about these types of scams, see this Office's publication called "Computer Scams." The types of security software needed to connect safely to the Internet and read email include:

   - Anti-virus software, which can stop email "worms" from infecting your computer.
   - Firewalls—an electronic brick wall—which help keep intruders out of your computer.
   - Anti-spyware software. Given the increasing sophistication of spyware, many experts recommend using two anti-spyware programs, which may offer more protection.
   - Email-scanning software that scans both incoming and outgoing email.
   - An anti-phishing add-on to your web browser, which can caution you to not visit unsafe websites.

3. **Use settings to your advantage.** Turn on auto-updates for your operating system and browser. Turn on the junk email filter. Report any spam that reaches your inbox. Set the email reader to read email in "plain text." Turn off automatic downloading of attachments.

4. **Trust your instincts.** Before opening an email, ask yourself whether you know the sender. Were you expecting an email? Delete spam without opening it. Never respond to spam or click a link in the message, even to "unsubscribe," because that only confirms to the spammer that you are a valid recipient and a perfect target for future spamming.

5. **Be wary of unsolicited email attachments, even from people you know.** Just because an email message looks like it came from your mom or your bank doesn't mean that it did. Viruses can "spoof" a return address, making it look like the message came from someone else. If possible, check with the person who supposedly sent the message before opening an attachment or clicking a link.

6. **If you must open questionable email, do not click links or open attachments unless you know your security is strong.** Does the email you've received pass the smell test? Is it full of misspellings? Does it ask for money, tell you that you are a winner, or offer you something too good to be true when you've never heard of the company before? If so, press delete! Never make a purchase from an unsolicited email.

7. **Many people have two or more email accounts, one for friends and family, and one or more other free, web-based accounts that might be misused by spammers.** If the accounts start to fill up with spam, get rid of them and open new ones.