

Avoid Email Scams

How to Avoid Email Scams

Your email is already filtered for spam. Because spam filters need to carefully avoid blocking real messages, some spam will get through. Your spam filter just reduces the volume of spam; you still need to be on your guard. Here are the most common hazards to watch out for:

Attachments

- Hackers can send attachments that contain malware that can steal your identity or take over your computer when the attachment is opened. Vulnerabilities in the program that opens the attachment can be exploited.
- Those dangerous attachments are often sent along with blank or vague messages so that you have to open the attachment to find out what the message is supposedly about. By then, the damage is quietly done to your computer.
- Some attachments are simply used to hide the spam message from the spam checker. It will contain fraudulent instructions for you to follow or misinformation for you to believe.
- An attachment in a vague or blank email message begs you to open it out of curiosity. Don't open attachments that are not well explained by senders that you trust.

Web Links

- Some web links look almost like the ones you trust. `usu.com` is not the same as `usu.edu` and `welsfargo.com` is not `wellsfargo.com`.
- Some web links look right but don't really take you to the web address you see. A "youtube.com" link may actually take you to "evilguys.com" if you just click on it instead of typing it yourself.
- Some web links contain the familiar information in the wrong place. `http://account.com/aggiemail.usu.edu` does not go to `aggiemail`.
- A cryptic web link in a vague or otherwise blank email message begs you to click on it out of curiosity. When you click, it's too late!

Free Offers aren't really Free. If they give you what you expect, they have probably taken something without telling you. They may take marketing or demographic data or personal information, or they may take some control of your computer - logging your keystrokes or using your disk storage or bandwidth for their own illegal purposes.

How can you protect yourself?

1. Be an Internet Skeptic
2. Disable any Preview or AutoRun features
3. Keep everything updated: Operating System, AntiVirus program, Adobe Acrobat, Flash, Word, Excel, etc.
4. Remember that email is not secure and not authenticated. It is easy to forge a sender address.