

9 Tips for Email Safety

1. **Don't open emails from someone you don't know or trust.** If it seems fishy, it probably is. Report the message as spam and move on.
2. **Avoid sending any sensitive information over email.** When you send a message, you no longer have control over what is done with it or to whom it is forwarded. Common email scams employ email messages and even websites that look official, but are in fact attempts to steal your identity to commit fraud. This is the activity commonly known as phishing. Sensitive information such as passwords, bank account numbers and social security numbers should never be sent via email. PayPal and your bank are examples of companies that would never ask for personal information in an email.
3. **Never open an attachment within an email from a company or person you don't know (or that you were not expecting).** Attachments may contain viruses, which can seriously damage your computer. Drag these emails to your spam folder.
4. **Never reply to or click on links inside spam emails.** Replying to, clicking on links within, or even unsubscribing from spam emails typically only informs the sender that they have found an active email address to which they'll send more spam emails. Instead, report the message as spam.
5. **Use a spam filter.** Spam filters help you keep spam emails from your inbox or flag spam emails as such so that you are aware of them. Depending on the software and configuration some spam filters can automatically eliminate junk emails and block web bugs that track your activity and system information.
6. **Use anti-virus software.** It is highly recommended that you install and maintain good and well-respected anti-virus software on your computer to prevent infection. Scan all email attachments with a virus program before downloading/executing any, even if they come from someone you know. Avira Antivirus is a good recommendation for an antivirus.
7. **Remember to log out/sign out,** especially if you're using a public computer, such as at the library or an Internet cafe, and close the browser. It's quick, easy, and may save your account from unwanted trespassers.

8. **Change your password frequently and don't share it with anyone.** It's recommended to change passwords at least every 60 days, particularly if you currently view and manage your email on a public computer. Use a mix of letters and numbers, as those passwords are harder to break. The password should not be easy to guess -- a common mistake is to use the company's name in the password or something generic such as "1234." Never share your password with anyone.

9. **Avoid unsolicited bulk mail.** Unsolicited bulk email messages can fill up your mailbox and become extremely frustrating. To avoid this predicament:
 - a. Don't give your email address to sites you don't trust.
 - b. Don't post your email address to public places online like message boards, comment boards, or even your personal website.
 - c. Keep your personal email private except from people that you really want to hear from. You can set up a second email account for registering for public Web sites.
 - d. Use an alternate email address when buying a product from a site for the first time or signing up for a new service.