

14 Tips for Using E-mail Safely

There is no doubt that using email safely is one of the top concerns of our customers. There are so many pitfalls and it's easy to make mistakes.

So, we've created a list of 14 practical tips for using email more safely:

1. Don't open attachments. The old advice was not to open attachments unless you knew the sender. However, that's no longer good advice since your friends can unknowingly send viruses, spyware and trojans if their computers are infected.
2. Use a firewall. Hardware or software firewalls can offer protection against hackers.
3. Install anti-virus software and use it regularly. This is critical -- anti-virus protection won't do you any good if you don't keep it updated or if you don't run regular scans. It's best to set up your anti-virus software to automatically install the latest patches and scan new files automatically.
4. If you use Windows, make sure you keep it up-to-date. Either visit Windows Update once a week, or you can set it up to automatically update itself.
5. Install anti-spyware software and use it regularly. Our advice is similar to anti-virus software -- you need to keep it updated regularly and run regular scans. For more info, visit our Anti-Spyware Resource Center for more info:
6. Stay up to date and use the latest versions of your email program and browser. These often contain the latest security patches.
7. Use plain text email rather than HTML formatting. HTML messages contain any type of formatting other than text (e.g., fonts, bolding, italics), and/or they can include graphic images or colors. Although HTML messages may be nicer to look at, viruses can be transmitted via HTML messages.
8. Don't use Microsoft Outlook or Outlook Express unless your employer requires it. These email programs simply contain too many security holes. We recommend you use one of these alternatives:

Thunderbird (PC or Mac)

<http://www.mozilla.org/products/thunderbird/>

Eudora (PC or Mac)

<http://www.eudora.com>

Pegasus Mail (PC)

<http://www.pmail.com>

9. If you must use Outlook or Outlook Express, be sure to read email in plain text. Here is what Microsoft advises on their website on their page titled "Increase Your Browsing and E-MailSafety":--- Begin Advice

VALLEY

COMPUTER RESOURCES, INC.

From Microsoft To help increase your e-mail security, set your e-mail program to read all messages you receive as plain text. To read messages in plain text in Microsoft Outlook Express:

1. On the Outlook Express Tools menu, click Options.
2. In the Options dialog box, click the Read tab.
3. Select the checkbox to Read all messages in plain text.
4. Click OK.

To read messages in plain text in Microsoft Outlook 2003:

1. On the Outlook Tools menu, click Options.
2. On the Preferences tab in the Options dialog box, click the E-Mail Options button.
3. In the E-Mail Options dialog box, select the checkbox to Read all standard mail in plain text.
4. Click OK to close the E-Mail Options dialog box, and then click OK to close the Options dialog box.

You can find Microsoft's other 3 suggestions here:

<http://www.microsoft.com/security/incident/settings.msp>

10. Change your passwords at least once a month. Make sure your password contains both letters and numbers and is not something obvious, such as a word in the dictionary, your birthday or your dog's name.

11. Never share your passwords. Scammers often try to seem like they are in positions of authority, and they insist you need to tell them your password. Don't.

12. Always log out of your email account and web browser, especially if you share your computer or are in a public place. If no logout is available, simply quit the application.

13. Never respond to spaham. As you know, one of our mottos is: "if it's spaham, it's a scam."

14. Back up your email regularly. If you do have a problem, at least you won't lose important email.