

Online Safety

Computers and the Internet have presented our world with unprecedented access to information more quickly than ever before. The benefits of such access to information, however, also present many dangers. Warnings exist everywhere and are communicated in many ways in order to make Internet users aware of as many dangers as possible.

Unfortunately, most of these warnings are written in a manner that only a computer “geek” can understand. In order to clear up the fog that generally surrounds online safety warnings, here are a few of the most important as related to other real-world warnings.

- **Don't trust candy from strangers** - Just because something is published on the Internet doesn't make it true. The Internet is open for anyone and everyone to publish their facts, opinions, ranting, sales gimmicks, etc. So, don't accept anything posted as fact unless you can verify that the source is reliable. Websites and email addresses can be easily spoofed, so verify all email addresses before opening unexpected attachments or responding to requests for information. Most reputable companies, especially government and financial institutions, will never send requests for your personal information via email.
- **If it sounds too good to be true, it probably is** – Most people have come across emails or Internet pop-ups that promise fantastic rewards or wealth beyond your dreams. Contrary to their claims, however, there are no wealthy strangers desperate to send you a piece of his or her fortune. Beware of promises such as these. They are most likely spam, hoaxes, or phishing schemes. Don't click on any associated links to websites or products, either. Spyware, adware, and viruses are often packaged with claims such as these since they are so enticing.
- **Don't advertise that you are away from home** – Most email accounts and programs today offer an “Out of Office Assistant” or other such autoresponder. These are great when used within the work place for letting your clients and other employees know that you are unavailable, but be careful with what accounts you use this with and with the wording. You do not want to let potential attackers know that you are going to be away from your home, or worse, give specific details about your vacation destination and itinerary. Instead of “I will be out of the country between...”, use phrase such as “I will be out of the office and not have access to email between...”. If possible, try to restrict what addresses the autoresponder can respond to as well. For every spam email that you receive while this is turned on, you are confirming with the spammer that your email address exists and is active so that he or she can spam you more and share your address with friends.

-
- **Lock up your valuables** – Most people would never leave their cars or homes unlocked while away. The same should be true with your computer. Take steps to protect your data and computer by following good security practices. Some of the most basic precautions include locking your computer while you are away from it (even short trips away), using firewalls, using anti-virus software, using strong passwords, and keeping your computer up-to-date with all updates.
 - **Have a backup plan** – Data can be lost from your computer in so many ways that backups are vital to the survival of your information. Very real risks of data being stolen, corrupted, changed, or lost due to hardware or software failures exist at all times. Regular backups of your information should be taken so that you will have clean, complete copies in case the worst should happen. Backups also help you identify what is missing or changed should the need for such information arise. Keep in mind that if you did not know your information was subjected to loss or corruption, the backups may be compromised as well. So, use a backup media rotation, if possible.

About Desktop Resources, Inc.

Desktop Resources, Inc. was founded in 1995 by Tony Schafer, and is a leader in helping organizations couple their business initiatives with the technology to address those needs. DRI's "InformIT" managed services offerings proactively manage client infrastructure and strive to prevent problems before they occur.

For more details, contact DRI at (317) 596-3650 or <http://www.DesktopResources.com>