



National Cyber Alert System

Cyber Security Tip ST05-014

[Archive](#)

Real-World Warnings Keep You Safe Online

Many of the warning phrases you probably heard from your parents and teachers are also applicable to using computers and the internet.

Why are these warnings important?

Like the real world, technology and the internet present dangers as well as benefits. Equipment fails, attackers may target you, and mistakes and poor judgment happen. Just as you take precautions to protect yourself in the real world, you need to take precautions to protect yourself online. For many users, computers and the internet are unfamiliar and intimidating, so it is appropriate to approach them the same way we urge children to approach the real world.

What are some warnings to remember?

- **Don't trust candy from strangers** - Finding something on the internet does not guarantee that it is true. Anyone can publish information online, so before accepting a statement as fact or taking action, verify that the source is reliable. It is also easy for attackers to "spoof" email addresses, so verify that an email is legitimate before opening an unexpected email attachment or responding to a request for personal information (see [Using Caution with Email Attachments](#) and [Avoiding Social Engineering and Phishing Attacks](#) for more information).
- **If it sounds too good to be true, it probably is** - You have probably seen many emails promising fantastic rewards or monetary gifts. However, regardless of what the email claims, there are not any wealthy strangers desperate to send you money. Beware of grand promises—they are most likely spam, hoaxes, or phishing schemes (see [Reducing Spam](#), [Identifying Hoaxes and Urban Legends](#), and [Avoiding Social Engineering and Phishing Attacks](#) for more information). Also be wary of pop-up windows and advertisements for free downloadable software—they may be disguising spyware (see [Recognizing and Avoiding Spyware](#) for more information).
- **Don't advertise that you are away from home** - Some email accounts, especially within an organization, offer a feature (called an autoresponder) that allows you to create an "away" message if you are going to be away from your email for an extended period of time. The message is automatically sent to anyone who emails you while the autoresponder is enabled. While this is a helpful feature for letting your contacts know that you will not be able to respond right away, be careful how you phrase your message. You do not want to let potential attackers know that you are not home, or, worse, give specific details about your location and itinerary. Safer options include phrases such as "I will not have access to email between [date] and [date]." If possible, also restrict the recipients of the message to people within your organization or in your address book. If your away message replies to spam, it only confirms that your email account is active. This may increase the amount of spam you receive (see [Reducing Spam](#) for more information).
- **Lock up your valuables** - If an attacker is able to access your personal data, he or she may be able to compromise or steal the information. Take steps to protect this information by following good security practices (see the [Cyber Security Tips index page](#) for a list of relevant documents). Some of the most basic precautions include locking your computer when you step away; using firewalls, anti-virus software, and strong passwords; installing appropriate patches; and taking precautions when browsing or using email.
- **Have a backup plan** - Since your information could be lost or compromised (due to an equipment malfunction, an error, or an attack), make regular backups of your information so that you still have clean, complete copies (see [Good Security Habits](#) for more information). Backups also help you identify what has been changed or lost. If your computer has been infected, it is important to remove the infection before resuming your work (see [Recovering from Viruses, Worms, and Trojan Horses](#) for more information). Keep in mind that if you did not realize that your computer was infected, your backups may also be compromised.

Authors: Mindi McDowell, Matt Lytle

Produced 2005 by US-CERT, a government organization. [Terms of use](#)

Last updated July 07, 2005