



# Security Awareness Tips

## Password Security

### **Don't share your password with anyone.**

While this seems like a very basic concept, many people don't consider it a security risk to share or give passwords to helpdesk technicians, co-workers, managers, friends, or family members. Remember... Your password is the key to your User ID, so don't let other people have access to it.

### **Don't write your password down.**

Passwords considered strong or secure are often too complicated to remember. For this reason, it's very tempting to write them down. It's always best to commit your password to memory. However if you must write something down, jot down a hint or clue that will help jog your memory or store the written password in a secure, locked place.

### **Change your password often.**

Even if you use a strong password, there is still the chance that someone could guess or crack it. For this reason, you should change your password often. Changing your password not only minimizes the chance that someone could guess or crack your password, it also shortens the length of time that person would have control of your system.

### **Use a different password for each of your accounts.**

Using a single password for each of your accounts would be comparable to using a single key for your car, your house, and your office. If someone steals your key (or gets your password), they have access to everything. Using multiple passwords requires additional effort on your part (you have to remember more) but it reduces the possibility that someone could gain access to all your

### **Don't check "remember my password" boxes.**

Numerous programs offer the option of "remembering" your password. Unfortunately, many of them have no built-in security measures to protect that information. Some programs actually store the password in clear text in a file on the computer. This means anyone with access to the computer can read the password. It's best to retype your password each time you log in eliminating the possibility that someone will be able to steal or use it.

## Desktop Security

### **Don't download files from unknown sources**

Not all web sites are safe. Always ensure that the source you are downloading from is legitimate. Use extreme caution if you are referred to a site by an email message. If you're uncertain, don't download.

**Lock your computer when you aren't using it.**

An unlocked computer is an open invitation to anyone that walks by. It would only take a few seconds for someone to delete important files or access sensitive information. Lock your computer when you aren't using it and if possible, shut it down when you leave each day.

**Use anti-virus software.**

Make sure you have anti-virus software installed on your computer and update it regularly. Out-of-date anti-virus software will not protect your computer from new viruses.

**Patch and update on a regular basis.**

Because hackers are constantly looking for vulnerabilities, it is important to keep your software up to date and patched. Unpatched out-of-date systems are a leading cause of security incidents. Take the time to ensure you have the most recent patches and updates installed.

**Backup important files on a regular basis.**

Backup important files on a regular basis and store the backups in a safe place. (Preferably off site.) You can backup files to removable disk or save copies to network shares. Unfortunately, it's not a matter of if you'll lose files (intentionally or unintentionally); it's a matter of when.

## Email Security

**Don't open unknown or unexpected email attachments.**

Just because you recognize the sender's email address (some viruses spread by using the address book of the victim) doesn't mean that the person actually sent the attachment. In addition, email can easily be forged to appear to be coming from someone you know. If you aren't expecting it, don't open it. If you think the attachment may be legitimate, contact the sender and verify that they did indeed send it.

**Don't send confidential information via email.**

Sending email is like sending a postcard. There's always the possibility that the email message could be intercepted, copied or read by people other than the intended recipient.

**Don't reply to unsolicited email messages (SPAM).**

By responding, you only confirm that your email address is active. Another thing you shouldn't do is click the "remove me" link in the message. Links in email can point to an IP address other than the one you think it references. The best thing you can do is delete the message.

**Turn off the message preview pane in Outlook or Outlook Express**

If the message preview pane is enabled, the messages in your inbox are automatically "opened" as you scroll through them. While this is convenient, it also poses a potential security risk. If you

disable the preview pane, you can delete any email that looks suspicious BEFORE it's opened and avoid a possible virus infection.

### **Don't be an unintentional Spammer.**

If you're like most people, you've probably received at least one hoax or chain letter in your inbox. What should you do with the next one you receive? Delete it! Why you ask? Because chain letters and hoaxes have the potential to cause problems (lots of network traffic or just filling up someone's inbox) and they can also be very annoying. Visit the following sites to find out more about hoaxes and chain letters.

<http://www.snopes.com>

<http://www.breakthechain.org/>

<http://hoaxbusters.ciac.org>

## **Protect Your Identity**

### **Don't fall for phishing schemes.**

Could you tell if an email message requesting personal information was legitimate? In most cases you can usually trust your instincts. (If an email message looks suspicious, it probably is.) However there are some messages that look like the real thing but aren't. If an email message contains any of the following phrases, there's a pretty good chance it's a phishing scheme.

- A. We need to verify your account information.*
- B. If you don't respond immediately, your account will be cancelled.*
- C. Click the link below to update your information.*

Take the Phishing Quizzes and see how good you are at identifying phishing schemes.

<http://www.washingtonpost.com/wp-srv/technology/articles/phishingtest.html>

<http://survey.mailfrontier.com/survey/quiztest.html>

### **Protect your Social Security number.**

Avoid using your social security number whenever you can. (Many places use social security numbers for user identification.) Ask to use an alternate number if possible. In addition don't print it on personal checks. Your Social Security number is the key to most of your financial information which makes it a prime target for criminals. Only give it out when absolutely necessary.

### **Make sure your personal information is protected when you do business online.**

Always read the privacy statement before you fill in the blanks. You should also verify that the site is secure before you submit any information -- look for https in the web address and for a padlock or key in the lower right corner of your browser. Don't send your personal information (social security number, credit card number, etc.) in an email or through instant messaging.

**Periodically check your credit report.**

Get a copy of your credit report from each of the three major credit bureaus every year. (Federal law gives you the right to one free credit report from the three credit bureaus: Equifax, Experian, and TransUnion -- <http://www.ftc.gov/bcp/online/pubs/credit/freereports.htm>.) Check the reports to make sure everything is accurate. Consider staggering the requests and obtain one report every four months. That way, you can watch for signs of identity theft (i.e. inquiries that were not generated by you, accounts you didn't open).

**If are a victim of identity theft, report it immediately.**

Here are some things you should do.

1. Contact the three major credit bureaus and have them place a fraud alert on your credit report.
2. If a credit card was involved, contact the credit card company and close the account.
3. Contact your local law enforcement agency and file a report.
4. File a complaint with the Federal Trade Commission.