The Web seems almost as vital to life as water. When was the last time you went three days without some kind of access to the Internet? But just as contaminated water can be harmful, there are risks associated with accessing online resources.

### General Precautions

#### Protect Your Social Security Number - Sharing it is like handing over the keys to your identity.

#### Protect Your Privacy - Know what information the site is collecting and how it is used. Find out if the site is sharing information. When filling out forms, enter only required information; leave optional fields blank.

#### Keep Passwords Private - Never share your passwords, change them frequently, and do not use the same password for multiple sites. Don’t display or store passwords on or near your PC.

#### Don't Email Personal/Financial Information - UA and other reputable institutions will NEVER ask you to send passwords or other secure information via e-mail.

#### Trust Your Instincts - If it doesn’t feel right, don’t do it. Be skeptical to a fault.

#### Look Over Your Shoulder - Always be aware of your surroundings and make sure that no-one in the real world can snoop into your online space.

### How to Be Cyber Safe

1. Protect your personal information. It’s valuable.
2. Know whom you’re dealing with online when using e-mail, IM, or social networking sites.
3. Keep your security software up to date.
4. Keep your operating system and Web browser up to date, and learn about their security features.
5. Keep your passwords safe, secure, and strong.
6. Back up your important files.
7. Learn what to do in an emergency. Contact the IT Service Desk at 348-5555 to report a computer security incident.

### Shopping and Investing

#### Know Your Merchant - Before placing an order with a vendor, check the Better Business Bureau, seller ratings, and the site’s privacy, security, and return policies. Make sure there is an alternate contact number in case something goes wrong.

#### Only Use Secure Websites - Shop and invest only on sites that offer an https:// connection. Another indicator that you are using a secure Web site is a padlock or unbroken key displayed in the browser.

#### Only Use a Credit Card - With a credit card, you have the right to dispute charges, which is not available with a debit or check card, bank checks, or cash. It also a good practice to use a single credit card for all of your online purchases.

#### Keep Good Records - Print your order and check against your credit card statement to ensure that your account was not used without permission.

#### Only Shop on a Secure Connection - You should never shop or bank online at a public kiosk or from an unsecured public wireless network.

### Social Networking

#### Don't Share Too Much - Be careful about how much personal information you post, including vacation plans.

#### Use Privacy Settings - Be mindful of privacy settings and keep information of new features that may affect your privacy.

#### Know Your Friends - Do not accept friend invitations from strangers.

#### Treat Others with Respect - Do not engage in cyber bullying or forwarding other people’s embarrassments, as you would not want that to happen to you. Respect and reciprocate the privacy of others.

#### Do Not Meet Friends You Make Online - The person you are talking to may not be who you think. If you do meet an online friend, do not go alone.

#### Make Sure You Are on the Real Social Network - Beware of phishing sites disguised as a social networking sites that can capture your login and wreak havoc on your account.

### Free Antivirus Protection on the UA Network

As a service to the UA community and as a means of self-protection, UA has contracted with McAfee to provide the latest McAfee VirusScan Antivirus software free of charge for students, faculty, and staff. To obtain the software, you can download it from [http://oit.ua.edu/oit/services/software-licensing/software-by-category-2/](http://oit.ua.edu/oit/services/software-licensing/software-by-category-2/) when you are connected to the UA network.

UA also runs McAfee’s ePO Agent, which updates McAfee Antivirus daily for all faculty and staff.