About 2.5 billion people are now connected to the internet. Most are conducting business, sending emails, researching, streaming video or audio, and staying in touch with friends or family. However, there are also the “bad guys”.

We are aware that there are many threats & dangers in our everyday lives and we layer our defenses to protect ourselves. For example, we lock our car doors, set the alarm on our house, and know to look both ways before we cross a street.

Online security is similar. We need to set up layers of defense in order to protect ourselves and our information against the threats of the online world.

This is a guide on the 10 most important security measures you should be taking in order to protect yourself online. It is designed to help you create a layered defense, and understand the resources available to you as a member of the UA Community.

The University’s Information Security Office is presenting you with the THINK! Campaign. Our goal is to help you understand the risks that come with using the Internet and the importance of practicing safe online behavior so you may protect yourself and your information from online threats.

The THINK! Campaign is about taking a moment to think before you connect to places online, share information with others, or even just click on a link. We are encouraging the UA community to be more vigilant about practicing safe online habits, as well as understanding that Internet safety is a shared responsibility not only on campus but in your individual lives at home and work as well.

Taking action to be safer and more secure online is important not only for yourself, but as a member of the University of Arizona and as a global citizen, your individual actions can make the online community safer for everyone.
## Security Building Blocks

Safe computing practices include a combination of how you technically protect your computer by using software and security settings, and the physical actions you take. You need both to really make a difference. If you consistently use strong passwords, but then leave your computer unlocked and unattended in public places, you are still putting your data in jeopardy. If you use anti-virus software but aren’t careful about replying to or forwarding suspicious looking emails, you still risk spreading a virus. These “Security Building Blocks” set a solid foundation for security and should function as a security checklist so you are able to protect your data. For further information on each topic as well as instructions on how to implement these steps, visit the accompanying links to our website.

### 1. Keep systems up to date with automatic updating.

An unpatched machine is more likely to have software vulnerabilities that can be exploited. For information on how to set up automatic updating go to: [security.arizona.edu/online-security#update](http://security.arizona.edu/online-security#update)

### 2. Use Stronger Passwords.

Passwords should be at least 8 characters, combining letters, numbers, and special characters. You should have a different password for each important account, and change them regularly. Never share your passwords or write them down. Instead, use a password manager to generate & save passwords for you. For more information on creating passwords go to: [security.arizona.edu/online-security#strongpasswords](http://security.arizona.edu/online-security#strongpasswords)

### 3. Install End Point Security Software — antivirus & anti-malware.

Sophos is an antivirus & anti-malware software suite that is available as a free download to all University members for Windows, Macintosh, & Linux. For information on how to install the Sophos End Point Security Suite go to: [security.arizona.edu/online-security#install](http://security.arizona.edu/online-security#install)

### 4. Back up your data. Twice.

Backing up your machine regularly can protect you from the unexpected. Back up twice, to an external drive and to an offsite location such as an online backup, to protect against fire, burglary, or water damage. For more information on backing up your data go to: [security.arizona.edu/online-security#backup](http://security.arizona.edu/online-security#backup)

### 5. Use Secure Wireless Connections.

When connected to the Internet, your data can be vulnerable. While on campus, always use UA WiFi when connecting to the internet. Whenever off campus, use the UA’s VPN to create an encrypted tunnel between your device & the Internet. For more information on how to secure your wireless connections go to: [security.arizona.edu/wireless](http://security.arizona.edu/wireless)

### 6. Email: Think before you click, open, or reply.

Ignore unsolicited emails, and be wary of attachments, links, and forms in emails that come from people you don’t know, or which seem “phishy.” Avoid untrustworthy (often free) downloads from freeware or shareware sites. If it’s unexpected or suspicious for any reason, don’t click on it. For more information on how to avoid being phished go to: [security.arizona.edu/phishing](http://security.arizona.edu/phishing)

### 7. Protect Sensitive Data.

Reduce the risk of identity theft by encrypting everything that contains sensitive information. For data you need to retain, use the encryption tools built into your operating system. Securely remove all sensitive data from your hard drive you no longer need. Watch what you share on social networks. Criminals can easily gather a lot of information that could help them gain access to more valuable data. Visit [security.arizona.edu/idtheft & security.arizona.edu/secure-social-networking](http://security.arizona.edu/idtheft & security.arizona.edu/secure-social-networking)

### 8. Secure your Mobile Devices.

Increase the security of your mobile devices by taking the same precautions you do on your computer. For details, visit [security.arizona.edu/mobiledevice](http://security.arizona.edu/mobiledevice)


Realize that you are an attractive target to hackers. Don’t ever say “It won’t happen to me.” Stay up to date on the latest developments for your operating systems. Signup for UA Phishing Alerts & check out the quarterly UA InfoSec Newsletter at [security.arizona.edu](http://security.arizona.edu) for all things security.