

The Center for Infrastructure Assurance and Security

Cyber Security Hygiene

Practices

Your data is valuable to criminals. They are constantly finding new ways to trick you into giving it to them. But, with a few simple practices you can make sure you're not their next victim.

Don't trust email attachments. Beware of "free" offers or software that says that it can speed up your computer. These may contain malicious software that can wreak havoc on your computer.

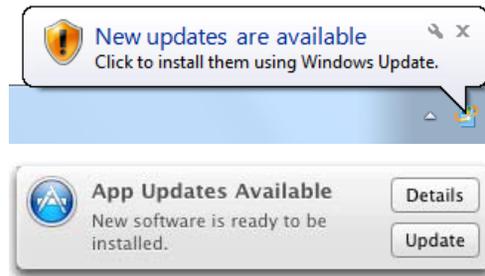
Look for signs that a website is safe. There are "bad" neighborhoods in the real world and the same is true in the cyber world. Software such as McAfee's SiteAdvisor or AVG's Security Toolbar, among others, can help notify you when a website isn't safe.

Consider encryption for sensitive data. Physical theft or loss of devices is very real risk. You can keep your data safe by encrypting it so that no thief can access your sensitive data. **A small investment in encryption can prevent a large expense in compromised information.**

Patches

New vulnerabilities are found every day in the software we use most often. Software vendors try to stay one step ahead of the attackers by patching or updating their software anytime someone finds a vulnerability. **You can take advantage of their hard work by applying those patches or updates to our system.**

When you see the following images, don't ignore them.



Passwords

Passwords are the first line of defense when protecting ourselves online. They are the equivalent to locks on our doors. Having a good password doesn't mean you won't be targeted. But not having a password or having a weak password almost certainly makes you vulnerable.



A good password doesn't have to be hard to remember. Here is one way you can create easy to remember passwords that can help keep you safe:

Choose a phrase of three or more words that is easy for you to remember but would be hard for someone else to guess. For example, *"I'll never turn off my firewall!"* This password is 32 characters long and would take a long time for an attacker to guess. For added complexity, add uppercase, numbers, and symbols. For example, *"strong passwords are cool"* could be *"strong-P@\$\$w0rds-ARE-Cool"*

Mobile Device Security

Do I need to backup my mobile device?

Yes. This may be more important than backing up your computer, as mobile devices are more likely to be lost. Think about the irreplaceable data contained on your mobile device — passwords, financial data, email, and social media information. Consider what your response would be if you lost all your photographs and contacts. If your digital life is in your phone, back it up.

Should I download that app?

Maybe, maybe not. There are a lot of factors to consider. Think about what data the application might be capturing and to whom it's sending that data. Think about the data and what it exposes about you — do they need to know your location?

Do they need that information about you? Do you want to give it to them? Is a free app still valuable to you if it infects your mobile device with malware? Bottom-line: make a deliberate and informed decision.

Do I need antivirus for my phone?

Probably. Just as on your computer, malicious software or malware exists for mobile devices. Emerging antivirus and security software



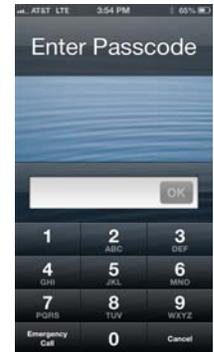
products for mobile devices can offer protection for the growing mobile device threats. The situation is different on iOS devices because Apple prevents malware in applications through their app store.

Should I use free or public Wi-Fi?

Maybe. Free and public Wi-Fi is akin to a public swimming pool. You're all playing in the same pool and subject to the effects of each person's personal hygiene. With free and public Wi-Fi, you have the good, the bad and the ugly when it comes to security. Is that a pool you really need to play in? There may be times when it's necessary, but consider carefully before accessing your sensitive information over free or public Wi-Fi. Make an informed decision and proceed with caution.

Should I lock or password protect my phone?

Absolutely! As our mobile devices become more linked to our daily lives they contain more and more important information and access. A locked device protected with a password or passcode can stop or slow down a potential issue. Be a more difficult target. So, put a password or passcode on your mobile device now.



About The Center For Infrastructure Assurance and Security

We are a team of cyber security professionals dedicated to advancing community and organizational security capabilities and collaboration. The Center for Infrastructure Assurance and Security (CIAS) has been called upon by the nation to strengthen cyber security preparedness in communities. We are part of The University of Texas at San Antonio and are committed to being the leader in the advancement of state and community cyber security.

What we do

Exercise Programs

The CIAS developed the world's only model for community cyber security preparedness. We customize our program to suit your organization or community.

Exercise Program Offerings

- Cyber Security Exercises
- Leadership Seminars
- Community Incident Response Planning
- Executive Cyber Security Awareness Seminars

Training

The CIAS offers low-cost training for cyber security. Our offerings include some of the most recognized certification training as well as courses not offered anywhere else.

Training Offerings

- (ISC)² CISSP Prep Course
- CompTIA® Security+ and Network+
- Voice and Data Security
- Planning Cyber Security Exercises
- Organizational Risk and Technical Assessments
- Community Dependency Mapping

Competitions

Known the world over for innovation in collegiate and high-school competitions, the CIAS develops and hosts national-level competitions that help forge the cyber security workforce of tomorrow. The CIAS develops realistic cyber defense competitions that are known as some of the most compelling events of their kind.



Contact us

Email: cias@utsa.edu

[@ciascybersec](https://twitter.com/ciascybersec)

4350 Lockhill-Selma, Suite 100, San Antonio, TX 78249 (210) 458-2119

<http://cias.utsa.edu>

