

THE WEAKEST LINK

That would be your password. First and foremost, NEVER give your password to anyone. ``Anyone" means your co-workers, your spouse, your systems administrator. In the event of an emergency, the sysadmin can change your password. Your systems administrator never has a need to know your personal password. If someone needs to get into your machine, and has a reason to be here, do not give them access to your account. Speak to the systems staff about setting up an account for them. Make your password something you can remember. Do not write it down. If you really, honestly forget your password, you can easily get a new one. In general, a good password will have a mix of lower- and upper-case characters, numbers, and punctuation marks, and should be at least 6 characters long.

HELPFUL UA RESOURCES

Security Incident Response Team

<https://www.sirt.arizona.edu/>

Securing Your Network at the UA

Email Network Operation at netops@arizona.edu or SIRT Team at sirt@arizona.edu or 626-0100

SANS Security Guides

<https://sitelicense.arizona.edu/sans/sans.shtml>

CCIT Business Continuity

<http://w3.arizona.edu/~bcis/BusCon.html>

UA Business Continuity & Disaster Recovery Standard

http://security.arizona.edu/Business_Continuity_and_Disaster_Recovery_Planning.pdf

USEFUL DISASTER PREPAREDNESS WEBSITES

Anti-Virus Links

<http://www.sophos.com>

<http://www.mcafee.com>

<http://www.symantec.com>

To download specific service packs and patches for a Windows operating system, go to Microsoft Windows Update site at:

<http://windowsupdate.microsoft.com>

Microsoft Office Downloads

<http://office.microsoft.com/downloads/default.aspx>

Corel Patches and Updates

<http://www.corel.com/servlet/Satellite?pagename=Corel2/Downloads/SupportDownloads>

Apple

<http://www.info.apple.com/support/downloads.html>

Linux Software

<http://software.linux.com/>

UA Site licensed Personal Firewall

<http://sitelicense.arizona.edu/kerio/kerio.shtml>

Disaster Recovery Journal

<http://www.drj.com/>

The Cert Coordination Center (CERT/CC)

<http://www.cert.org>

All comments, suggestions or questions should be sent to

Business Continuity and Information Security

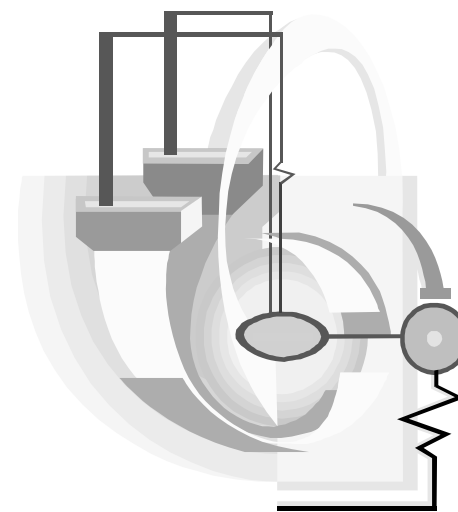
bcis@u.arizona.edu

Phone (520) 621-4482

Fax (520) 626-8346

<http://security.arizona.edu/>

RISK REDUCTION: *Computer Protection and Prevention*



THE UNIVERSITY OF
ARIZONA®
TUCSON ARIZONA

BACKUP YOUR DATA

Backing up your data regularly is vital insurance against a "data catastrophe." Unfortunately, this is a lesson that most people learn only from bitter experience.

Developing a solid backup plan requires some investment of time and money, but the cost is far less than the often-impossible task of recreating data for which no backup exists!

Perform a daily backup of important files to a local removable device – i.e., zip drive, CDRW or tape cartridge. Try to avoid using diskettes as they have a small capacity.

At a practical level, backing up your email files, word processor files, databases, web bookmarks, and any other files you directly create will provide you with sufficient backups to make recovery possible in the event of a crash.

Backup procedures in a server environment would mean that users would be saving data to an identified location on a departmental server. Daily incremental or differential backups would be performed along with a weekly full back of the entire server.

Offsite storage for your backup media protects the data in the event that the computer itself is destroyed due to a disaster in or around the area where servers are located.

KEEP YOUR OPERATING SYSTEM UPDATED

Having security built into your operating system is another feature of risk reduction. Operating systems such as Windows 2000/XP, Linux, Solaris etc, can provide complete protection of files on a stand-alone system (Files, folders, and applications can be made "invisible" to specific users).

Using file level permissions, computers can be configured to restrict access to system files and data. This prevents malicious users from deleting system files or damaging business applications. With these features, a single PC desktop system can be shared by multiple users and still maintain security for all files on the system.

PHYSICAL SECURITY

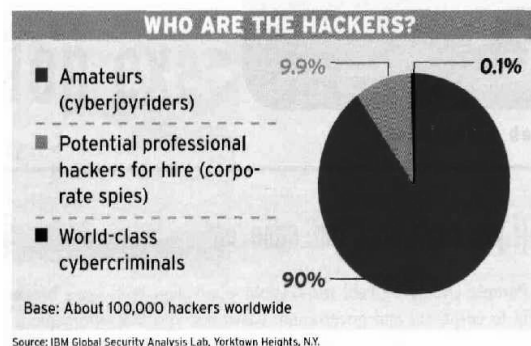
Critical data must be protected from threats such as unauthorized physical access, theft, or destruction.

- Place servers in a locked room.
- Lock down your monitors and desktops to your desk area with computer locks.
- Do not leave computer logged in if you are away for extended periods of time.
- Disable floppy boot ability via the Bios

WHAT IS A FIREWALL?

A personal firewall ensures that your personal computer is protected from malicious hackers and other intruders while preventing unauthorized access from your computer to a network. In essence, a personal firewall makes your protected computer invisible to the outside world. It also protects your computer by actively looking for hostile intruders and Trojan Horse applications. If an intrusion attempt occurs, the personal firewall detects it in real-time with a built-in host and application based intrusion detection technology, while blocking it by default.

The graphic below shows that amateur hackers are by far the biggest threat on the Internet at the current time. They are responsible for about 90% of all hacking activity.



For more on these statistics go to:

<http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm>

UNINTERRUPTABLE POWER SUPPLY (UPS)

Install a UPS wherever continuous power is essential to daily operations, like in a server room. In case of a power failure, a UPS provides clean power with the capability to ride through power failures and give staff ample time to power down their computers and protect servers in the event of a total loss of electricity.

WHAT IS SOCIAL ENGINEERING?

Be careful whom you give information to. Attackers using social engineering techniques often use the telephone to convince network users that they are trusted partners, such as co-workers, information technology staff, or supervisors. These "trusted partners" often gain access to your computer or network by simply asking you for your password to gain access to your confidential data which can then be compromised.

CYBER TERRORISM

Here are a few key things to remember to protect yourself from cyber-terrorism:

- All accounts should have passwords and the passwords should be unusual, difficult to guess.
- Check with vendors for operating system patches, service packs and upgrades for network configuration. For Microsoft users go to: <http://windowsupdate.microsoft.com>
- Install service packs and hot fixes to a server before exposing it to the network. See notation ** below.
- Audit systems and check logs to help detect and trace an intruder.

If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble.

** For more info on the different types of updates go to: <http://www.infosecuritymag.com/2002/jun/surgeongeneral.shtml>