IT TIMES

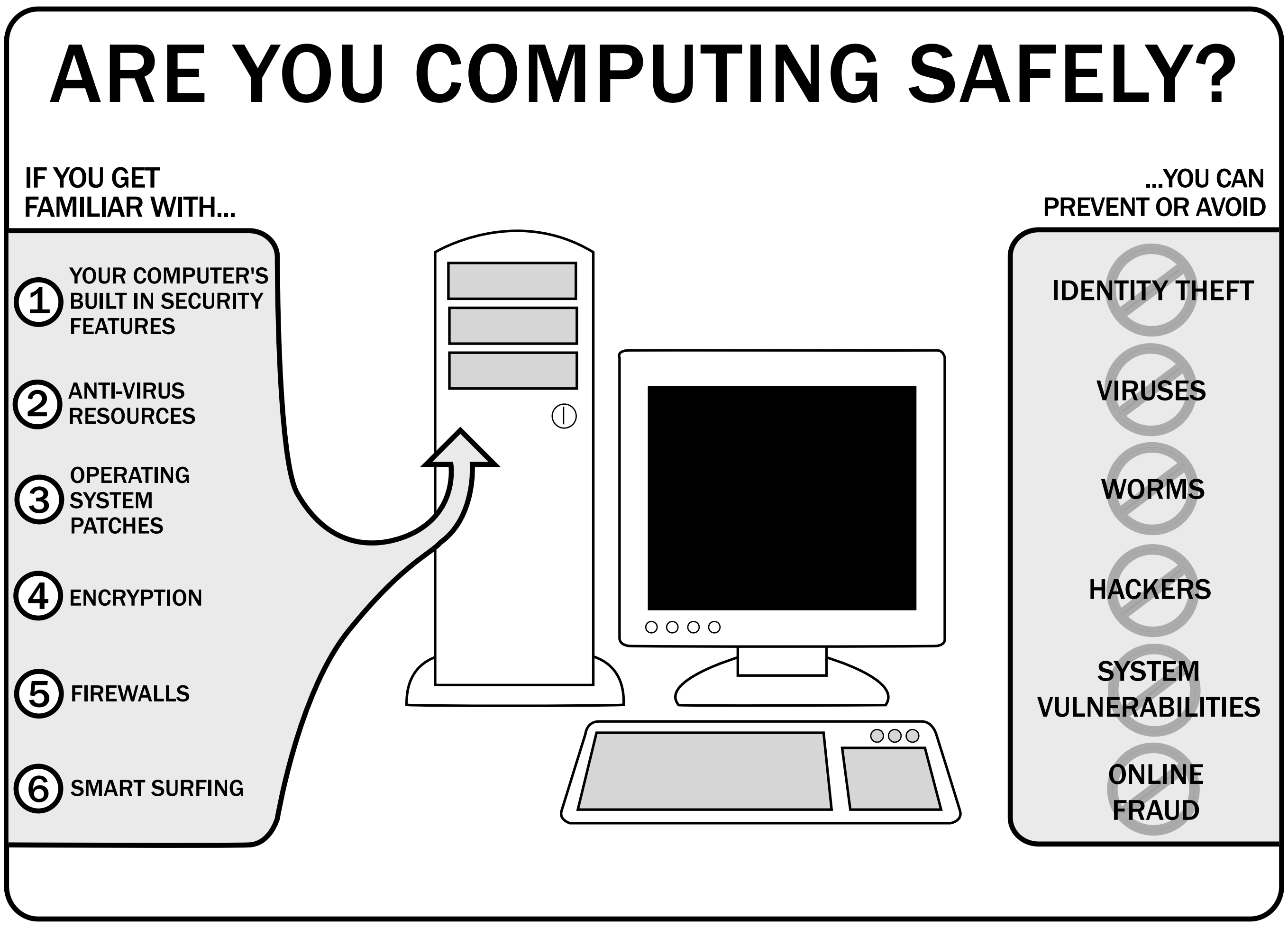
Information and Educational Technology News for UC Davis

Special Edition March 2004

http://technews.ucdavis.edu

SPECIAL EDITION

No doubt, you have already received at least a few spam email messages and dealt with the aftermath of a computer virus or two. If not, you probably don't use a computer very often. Security concerns grow as opportunists learn new ways to exploit technology for a variety of hacking and thieving purposes. In this edition of IT Times we offer you some basic instructions for safeguarding your computer. Though it is easy to become overwhelemed by advice about all the ways you should protect yourself from hackers, viruses and identity thieves, you still can't afford to be in the dark about computer security. For this reason, we hope you'll find this issue helpful. While the campus continues to find solutions to widespread system vulnerabilities, your best bet is to arm yourself with knowledge about the latest security measures. After all, protecting your computer is your responsibility. Read on and don't forget to visit the campus Computer and Network Security Web site regularly at security.ucdavis.edu.



ARE YOU COMPUTING SAFELY?

IF YOU GET FAMILIAR WITH...

1 YOUR COMPUTER'S BUILT IN SECURITY FEATURES

2 ANTI-VIRUS RESOURCES

3 OPERATING SYSTEM PATCHES

4 ENCRYPTION

5 FIREWALLS

6 SMART SURFING

...YOU CAN PREVENT OR AVOID

IDENTITY THEFT

VIRUSES

WORMS

HACKERS

SYSTEM VULNERABILITIES

ONLINE FRAUD

What To Do When Your Name Escapes You

A Primer on Identity Theft Prevention

Six months after moving to a new house, Blythe found out that the new tenants in her old apartment were using her personal info (copied from her unforwarded mail) to get free cable and other costly services for the apartment. Jeff discovered, after receiving congratulations from a family member on his "new venture," that someone had used his Social Security number to get a business loan. Thieves broke into Regina's house while she was on vacation and left all of the electronics and other easily-fenced items, stealing her credit files and personal information instead.

Why would thieves go for paper instead of material goods? Now that most products and services can be purchased using credit card numbers or account codes, thieves go straight for the numbers.

Whether identity theft occurs when you lose your wallet or when you let information slip into cyberspace, it is one of the most insidious contemporary high-tech crimes. According to the 2003 Consumer Fraud and ID Theft Report, the Federal Trade Commission (FTC) received 214,905 ID theft complaints in 2003, up almost 33% from 2002.

What is Identity Theft?

Identity theft occurs when someone uses your personal information (i.e., your name, Social Security number, credit card number or other identifying information) without your permission, usually to commit fraud or other crimes. Thieves often pick up your info from computer systems or Web sites that do not employ the tightest security measures.

Victims of identity theft often have to spend lots of time –many months or years– and money cleaning up their personal and financial records. In the meantime, they may be refused loans, housing or cars, or even get arrested for crimes they didn't commit.

Ways To Minimize Risk

While there isn't a sure-fire way to prevent your personal information from being used illegally, there are a number of things you can do to guard against identity theft (see the sidebar on the right for some quick tips).

What the Campus is Doing About Identity Theft

Both the state government and the UC Davis administration have taken steps to respond to the growing problem of identity theft. On July 1, 2003, a new law went into effect in California that requires organizations to notify state residents when a computer security breach has permitted the release of personal information to unauthorized recipients. Shortly thereafter, the UC Davis administration, working with a team led by campus IT Security Coordinator Robert Ono, developed and released a detailed notification plan for the campus. In related letters to the campus from Provost and Vice Chancellor Hinshaw and Vice Provost for Information and Educational Technology (IET) John Bruno, campus units were encouraged to take "aggressive action" to protect against identity theft. To read the full message, visit directives.ucdavis.edu/2003/03–097.cfm.

Additionally, IET is working with the campus to explore encryption tools for campus use. Encryption "scrambles" sensitive information stored on computers so intruders cannot read it.

What To Do if You're a Victim

With time, persistence, backtracking, investigation and a whole lot of patience, Regina, Blythe, and Jeff were all able to clear their good names. If you've been a victim of identity theft, there are a few key steps you need to take, according to the FTC.

First, place a fraud alert on your credit reports and review them for accuracy, closing any accounts that have been tampered with or opened fraudulently. Next, file a report with the police in the community where the identity theft took place (you may need a copy of your report to validate your claims to creditors). Finally, you should file a complaint with the FTC.

You can call the FTC's Identity Theft Hotline toll-free at 1-877-IDTHEFT (438-4338). Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result. In addition, the FTC, in conjunction with banks, credit grantors and consumer advocates, has developed the ID Theft Affidavit to help victims of ID theft restore their good names. This form is available online at www.consumer.gov/idtheft/. ⚠

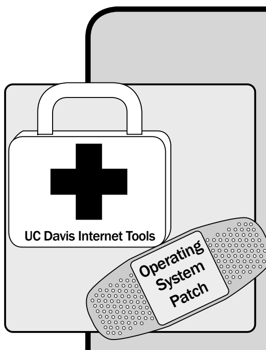
! Safety First

SECURE YOUR IDENTITY

- Order a copy of your credit report from each of the three major credit bureaus (You can find these at www.consumer.gov/idtheft). Make sure the reports are accurate and include only authorized activities.
- Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.
- Secure personal information in your home, especially if you have roommates, employ a housekeeper or are having service work done in your home.
- Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal procedures for those records as well.
- Don't keep personal identification stored on computers unless it is encrypted.
- When discarding documents containing personal identification information, use a shredder or mark over the sensitive information so it can't be read by dumpster-divers.
- Don't send personal identity information via email – it can be easily read or intercepted.
- When shopping online, make sure the site is secure. Before submitting your personal identity info to a Web storefront, look for the padlock icon in the corner of the page. You should also read the store's privacy statement – can the store resell or share your information with others without your permission? If so, they might not be worth your business.
- Visit security.ucdavis.edu/id_theft.cfm.

Some info here is taken from "ID Theft: When Bad Things Happen to Your Good Name" www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

VIRUSES AND WORMS



What are they?

Malicious small programs that easily replicate themselves, infect your computer, and often spread to others' computers via email attachments or network traffic.

What risks are involved?

Virus programs can delete files, format disks, attack other computers or just make your system run slowly. They can also create a "back door" that allows hackers to run programs on your computer or access your files.

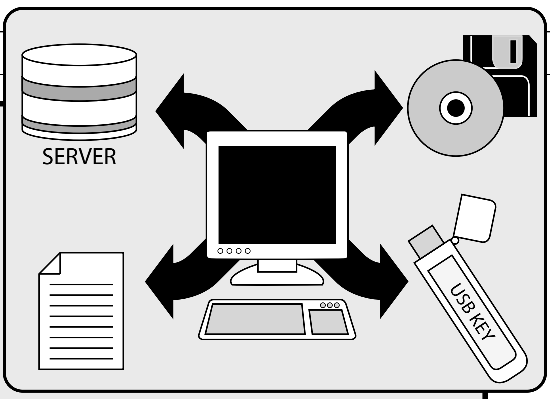
What can I do to protect my computer?

- Install anti-virus software on your computer and run daily updates. Anti-virus software is available on the UC Davis Internet Tools CD, which can be purchased at the Bookstore Computer Shop for less than $5. You can also download the software from the MyUCDavis Web portal by clicking on the "UCD Resources" tab.
- Pick up "patches" at your operating system's Web site to keep your computer fortified against possible attack.
- Reduce potential harm of a virus or worm infection by frequently backing up all of your files.
- Since 87% of viruses originate and transmit themselves via email, do not open email attachments with suspicious subject lines, file names, or messages. Some viruses can forge themselves to appear as if they are from someone you know; therefore, the "from" line alone cannot be trusted.
- Be aware that viruses may come to you in links sent via Instant Messaging, email attachments, infected disks, freeware, or file-sharing.

What is UC Davis doing to protect me?

Virus-filtering software checks every incoming and outgoing @ucdavis.edu email message for viruses. Widely-recognized viruses will automatically be filtered out of your incoming email. New viruses may still sneak through until the filter is trained to recognize them, which usually takes no more than 24 hours.

REGULAR DATA BACKUPS



What is it?

Creating a second copy of your computer's files on a consistent basis.

What risks are involved?

If you don't back up your data, you run the risk of losing it. Your files could disappear due to a virus, computer crash, accidental keystroke, theft, or external disaster.

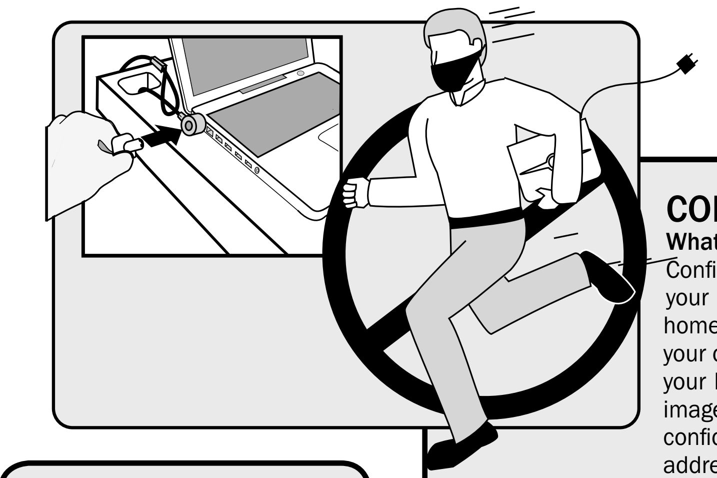
What can I do to protect myself?

- Back up critical and essential files on a daily basis and non-critical files on a weekly or monthly basis. You can back up your data to a CD, MySpace (available at my.ucdavis.edu), to a commercial online back up service (for a small monthly fee), flash drive, USB key, or to a server, if you can get access to one from your Internet Service Provider or commercial vendor. Some companies offer automatic backups when you purchase their programs.
- Keep all of your critical files in one place so you can easily create a duplicate copy.
- Store your backup media (CDs, disks, backup server, etc.) in a safe and secure place away from your computer, in case of fire or theft.
- Periodically test the capability to restore from the backup media. It's of little value to have a backup that is unreadable.
- On campus: Check with your department's tech support person to find out if he or she runs regular backups of departmental computers.

Safety First

Are you protecting your computer?

http://security.ucdavis.edu



INSTANT MESSAGING

What is it?

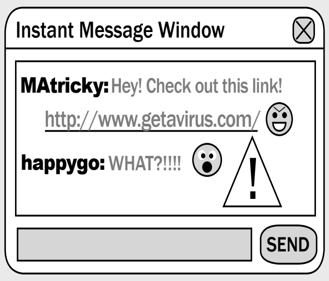
Instant messaging is available via a number of software programs, allowing you to type messages to classmates, colleagues, family and friends. IMing is popular because it is so convenient and because the messages are delivered in real-time.

What risks are involved?

Viruses can be very easily transmitted via instant messages containing files or links. IM programs, like all software, may also contain bugs and flaws that could compromise your computer. Because IMs are not encrypted, there is always the possibility that a third party is monitoring your messages.

What can I do to protect myself?

- Update IM software when the latest versions are released.
- Do not share identifying information, such as your credit card or social security numbers, over IM.
- Reset your password often.
- If you are programming-savvy, try using an open-source IM program such as Gaim or Fire, which tend to have fewer security flaws.
- If a stranger or a friend requests that you check out a URL, don't click on the link unless you know exactly what it is (chances are it's infected).



MAtricky: Hey! Check out this link! http://www.getavirus.com/

happygo: WHAT?!!!!

CONFIDENTAL DATA STORAGE

What is it?

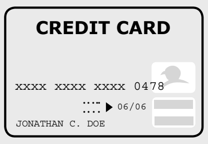
Confidential data is any information you don't want others to obtain without your permission including (but not limited to): Social Security number, home address, phone numbers of friends/family/colleagues/students, your drivers license or bank account numbers, a list of all your passwords, your home address or phone numbers, your employee ID number, digital images, word documents containing personal text, etc. Most people store confidential data of some kind on their computers within Word files, address books, or application settings.

What risks are involved?

If unauthorized persons steal or gain access to your computer and any of the confidential information you are storing, they could use that information to commit identity theft, the fastest growing crime in the U.S. (see page 1). Another risk is that the information could be changed and you may not immediately discover the unauthorized modification.

What can I do to protect myself?

- Minimize the amount of confidential information you store on your computer.
- Store the confidential information on portable media, such as a CD, flashdrive, ZIP disk or floppy disk. Secure the portable media in a locked cabinet when it is not being used.
- If you must store credit card numbers, Social Security numbers, or other confidential data on your computer, learn how to encrypt the files via some operating systems. (See the chart on page 4.)
- Physically secure your laptop or desktop computer to the desk where it sits. You can purchase a simple cable lock (similar to a bike lock) at any tech-supply store for around $30 that will deter and usually prevent theft.
- Set your computer to ask you for an account password at login. If someone else is sneaking onto your computer, this will prevent them from gaining access to your files. Be sure to disable the "Guest" account, as use of this account is likely to be untraceable.



What is UC Davis doing to protect me?

- UC Davis provides guidance for faculty and staff who have to store confidential data on their work computer. Visit security.ucdavis.edu/id_theft.cfm.
- Consult your department tech support person for finding ways to store confidential data.

SHOPPING ONLINE

What is it?

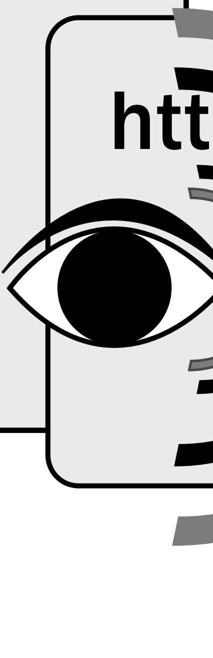
Almost anything can be purchased online if you have an Internet connection and a credit card.

What risks are involved?

If the site you're shopping on doesn't use data-security methods (such as encryption), your credit card or identity information could be transmitted into cyberspace, making it available to identity thieves. Illegitimate businesses could sell your personal information to other businesses or spammers, compromising your privacy.

What can I do to protect myself?

- Look for the padlock icon (usually in the lower corner of your Web browser), indicating the site is encrypted and that your personal information is protected as it moves between your browser and the site's Web server.
- Look at the URL of the site. In "https://" the 's' means SECURE data transmission.
- Read the site's privacy policy. Most legitimate businesses promise not to sell your personal info to other vendors. If you can't find the privacy policy, consider this as a strong danger signal.
- Don't buy if they don't offer you a way to print a receipt.
- Consider how reputable the store is since you are trusting them to safeguard your name and credit card number.



REPORTING SECURITY INCIDENTS ON CAMPUS

What is a security incident?

A security incident occurs any time your computer or personal information has been compromised, whether it involves theft, hacking, a vicious virus, or unauthorized use of campus network access. Anytime you are witness to an inappropriate or offensive use of campus email or networks, you should report the incident, or seek help and advice from campus technologists.

Why should I report a security incident?

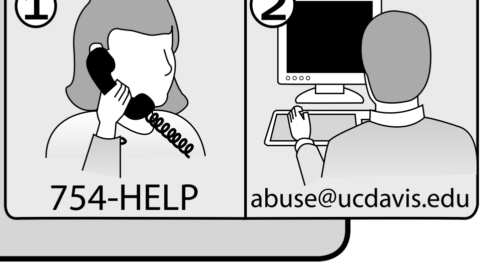
If your system has been infected or any personal data has been lost, campus resources can help you clean up the mess. Furthermore, as a user of the campus network, you should be aware of your rights and responsibilities.

How do I report a security incident?

- Know your rights as a campus computer user by reviewing UCOP's Electronic Communications Policy, which details appropriate uses of email and campus Web resources. See www.mrak.ucdavis.edu/web-mans/ppm/310/310-16.htm.
- Report security violations on campus to abuse@ucdavis.edu.
- Report computing problems to the campus computing help desk, IT Express: ithelp@ucdavis.edu or 754-HELP.
- Other campus technologists who may be alerted to security breaches (depending on the violation) might be the Business Contracts Office, the campus police, or Student Judicial Affairs.
- Periodically check the Computer and Network Security Web site (security.ucdavis.edu) for security alerts, or announcements about current virus outbreaks and prevention measures.

What else is UC Davis doing to protect me?

- UC Davis is developing an Incident Response Plan that will streamline the process reporting and responding to security violations. Visit the Computer and Network Security Web site (security.ucdavis.edu/report.cfm) to access the latest information and instructions for reporting security incidents.
- Check out the Security Incidents page of the Security Web site at security.ucdavis.edu/report.cfm.



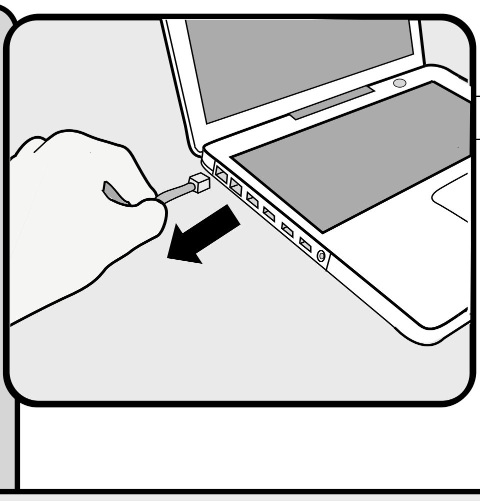
WIRELESS NETWORK

What is it?

The freedom to browse the Internet while sitting at your favorite café or tanning yourself on the UC Davis quad. Wireless networks are sprouting up everywhere, including UC Davis.

What risks are involved?

Because wireless access points don't require a user to plug into a port, the networks are often more difficult to monitor and secure. Many off-campus wireless areas won't require you to sign in with a username and password. If you're buying things online or logging on to Internet applications, it's a lot easier for someone to record your keystrokes and steal your identity.

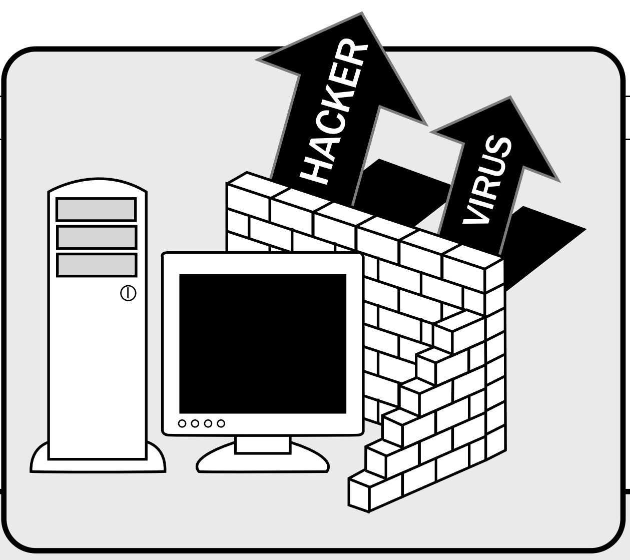


What can I do to protect myself?

- Restrict your online shopping to wired connections or to encrypted web browsers.
- Don't open programs that contain identifying information while you're on a wireless network. In fact, don't keep your Social Security number, driver's license number or bank account numbers anywhere on your computer, period.
- Keep your computer secure by applying operating system corrective patches when they are released by the software manufacturer and keeping your anti-virus programs up to date. Other computers using the wireless connection could be infected or compromised and may attempt to spread virus infections or to hack into other computers using the wireless network.
- Disable file sharing on your computer so that others can't help themselves to files on your computer.

What is UC Davis doing to protect me?

- The UC Davis wireless network fends off rogue surfers by requiring a login by all users. If you don't log in with a UC Davis username and password, you don't get access.
- UC Davis implements filters between the campus wireless network and the rest of the campus computing network to limit some of the more malicious attacks from emanating to or from the wireless network.
- UC Davis has a wireless resources Web page that will inform you about its policies and educate you before you decide to unplug. Visit wireless.ucdavis.edu.



FIREWALLS

What are they?

A firewall acts as a protective barrier between your computer and the Internet, monitoring all incoming and/or outgoing traffic and allowing only the network traffic you permit. Firewalls come in the form of software that nestles itself between your operating system and your network card. They also come in the form of hardware; for many home and small office users, it is a simple router device that sits between the network jack on your computer and the network wall connection. You can customize the level of protection the firewall gives you, setting it to filter information flow from specific domain names, addresses or types of network traffic.

What risks are involved if I don't have a firewall?

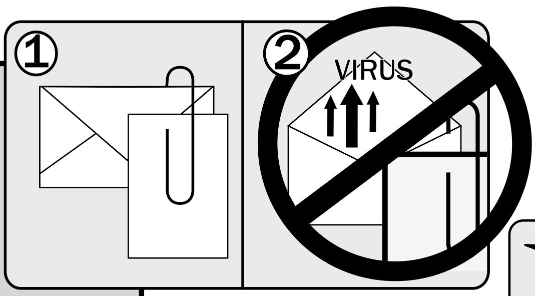
If your computer, like most, is automatically set to enable file sharing or to keep network ports open while you are online, you could be susceptible to a variety of attacks. If you don't have a firewall, which will monitor ports to stop unwanted traffic from slipping through, you have to know how to manually close ports and disable file sharing, in order to control risky traffic from coming in to your computer.

What are some of the disadvantages of installing a firewall?

If you use a firewall, you have to decide which kinds of network traffic to permit through the firewall. It is not always easy to determine which kinds of traffic are safe or unsafe. Also, like any add-on to your computer, a firewall can interfere with other applications on your system, making it difficult for the average user to troubleshoot any problems that arise. Firewalls are not failsafe, either. They may let malicious programs (disguised as friendly ones) slip through. Firewalls may also prevent campus vulnerability scanners from alerting you of a problem on your computer. Lastly, there may be restrictions on the use of personal hardware firewalls/routers, depending on which department or network you belong to on campus. If your computer comes with basic firewall capability or if you are thinking of installing a firewall, you should contact your tech support person first.

What is UC Davis doing to protect me?

- UC Davis is currently exploring ways to provide campus departments with an economical firewall solution. To find updates on the progress of this project, visit security.ucdavis.edu.
- If you are a departmental LAN administrator, you can find a list of benefits and caveats as well as installation tips and considerations at security.ucdavis.edu/fwresource.cfm.



EMAIL ATTACHMENTS

What is it?

A virtual package sent via email, usually a Word document from a colleague, or a photo from a friend.

What risks are involved?

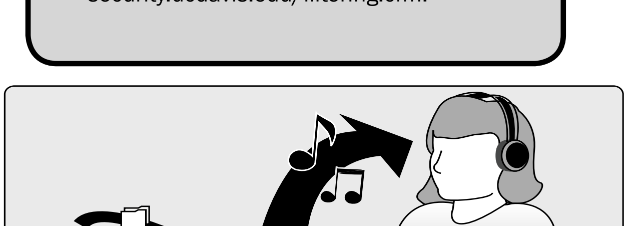
Sometimes the attachment isn't so friendly: it could be a document that, upon opening, loads a virus onto your hard drive. Some infected attachments could bring your whole system down by causing a hard-drive crash; others could open a port for hackers to invade your system. Some are designed to gnaw their way into flaws in your operating system. Some viruses are so smart that they attach themselves to emails from people you know and trust, tricking you into thinking the attachment is safe.

What can I do to protect myself?

- Install anti-virus software on your computer and update it daily. It will catch a majority of infected attachments.
- Do not temporarily disable anti-virus software on your computer – it's too easy to forget to re-enable the software.
- Keep your computer updated with the current security patches as infected email attachments may attempt to exploit program vulnerabilities.
- Just don't open attachments unless you are certain of the sender AND the contents of the attachment.

What is UC Davis doing to protect me?

- The UC Davis email servers automatically filter any known viruses from your email, but that doesn't account for brand new viruses yet unknown by the filtering mechanism. For more info on campus virus filtering see security.ucdavis.edu/filtering.cfm.



FILE SHARING

What is it?

Swapping music, movies, games, and other media with other users on a local network or peer-to-peer (P2P) program online. Examples of P2P programs include Kazaa, Morpheus, and Napster.

What risks are involved?

In addition to downloading viruses that shared files could contain, you could be breaking national copyright laws. Thus, not only might you infect your computer, you might also put yourself at risk for lawsuits and hefty fines. You may also be downloading spyware– software that gathers personal information about you without your knowledge, allowing hackers to access your personal files and programs, putting you at risk for identity theft.

What can I do to protect myself?

- Keep your anti-virus program updated and install the latest security patches on your operating system.
- Use freeware and shareware only from sources that you trust. Scan anything with your anti-virus software before installing it on your computer. Be wary of executable (.exe) files since they install immediately on your computer before you have a chance to scan them for viruses.

What is UC Davis doing to protect me?

- The campus offers anti-virus software, available for download via the "UCD Resources" tab in MyUCDavis or on the UC Davis Internet Tools CD, available at the UC Davis Campus Bookstore for less than $5.
- Legally, UC Davis can't protect you if a copyright-holder sues you for trading or downloading their property (songs, movies, software, etc.). It is your legal responsibility to respect copyright agreements on file-sharing networks. See the UC's copyright education Web site at www.universityofcalifornia.edu/copyright/.

UCDAVIS

WHAT THE CAMPUS IS DOING ABOUT COMPUTER SECURITY

DEPARTMENT FIREWALLS

In February 2004, a revised version of the Departmental Firewall Guidelines and Procedures document was released. The document is available from the Computer and Network Security Web site, or access it directly at security.ucdavis.edu/FWProcs.pdf. In addition to this document, a section of the Security site is dedicated to firewalls (security.ucdavis.edu/firewalls.cfm), providing general information about firewalls and links to additional resources.

FILE ENCRYPTION

In response to new federal and state laws protecting personal information, a workgroup was formed (in December 2003) and tasked with defining the requirements for file and disk encryption that can support the campus' academic, research and administrative needs. Recommendations are expected by March 31, 2004. See security.ucdavis.edu/sec_projects.cfm for additional information.

IDENTITY THEFT PREVENTION

With the passage of California Civil Code Section 1798 came the responsibility for notifying state residents when personal information is believed to have been obtained by an unauthorized source. A notification process is in place, and a section of the Computer and Network Security Web site has been dedicated to providing identity theft prevention information and victim resources to the campus community (security.ucdavis.edu/id_theft.cfm).

INCIDENT RESPONSE

A campus Incident Response Team has been created and charged with reporting, analyzing, prioritizing, investigating and responding to computer and network security incidents. Additional information is available at security.ucdavis.edu/sec_projects.cfm.

LUNCHTIME DISCUSSIONS

The campus IT Security Coordinator is working with a variety of technology vendors to develop opportunities for campus technical staff and other interested personnel to discuss new and ongoing security-related issues. Additional information about these discussions, including scheduling and agendas, is available at security.ucdavis.edu/training.cfm.

SPAM FILTERING

In May 2003, the campus implemented spam filtering on all campus email servers. This is an opt-in service, which means campus community members must sign up for the service by visiting email.ucdavis.edu/secure/spamfilter.pl or by opting in when they register for a new campus email account. For additional information about the campus spam filtering service and other spam filtering options, visit security.ucdavis.edu/spam.cfm.

VIRUS SCANNING

In July 2002, the campus implemented virus filtering on all of the campus email servers. Virus filtering continues, preventing millions of virus-infected email messages from entering the campus computer network each year. Additional information is available at security.ucdavis.edu/filtering.cfm.

VULNERABILITY AND INFECTION SCANNING

As a result of the recent proliferation of computer system vulnerabilities, a workgroup has been tasked with identifying a process by which existing vulnerability scanning method (which have already prevented significant damage to the campus network) can be deployed as a more proactive tool in the future. Recommendations are expected by March 31, 2004. Additional information is available at security.ucdavis.edu/sec_projects.cfm.

Are you taking advantage of the security features in your operating system?*

Are you taking advantage of the security features in your operating system?*	Windows 98/ME	Windows 2000	Windows XP	Apple OS X	Red Hat 9.x
OPERATING SYSTEM UPDATE NOTICE Your computer sends a message reminding you to visit a Web site and download important updates to your OS.		👍	👍	👍	👍
AUTOMATIC OS UPDATE INSTALLATION As long as you are connected to the Internet and click "OK," the updates are installed for you.	🖱	🖱	👍	🖱	
ACCOUNT LOGIN PASSWORD Requires a password each time your computer starts up, keeping others from misusing your computer.		🖱	🖱	🖱	👍
GUEST ACCOUNT PASSWORD Requires all users of your computer to login with their own accounts and passwords.		👍	👍	🖱	👍
SCREEN TIME-OUT PASSWORD Requires that you re-enter your password to get your computer out of sleep or screen-saver mode, keeping others from misusing your computer if you leave it unattended.	🖱	🖱	🖱	🖱	🖱
PASSWORD COMPLEXITY Demands that passwords include combinations of numbers and letters, which are more difficult for outsiders to crack.		🖱	🖱		👍
SECURITY ACCESS LOG Allows you to log certain security "events" of your choosing (e.g. login attempts, password failures, cd-rom usage, etc.), so you can track how your computer is being used by others.		👍	👍	👍	👍
ACCOUNT LOCKOUT Locks up your computer entirely if multiple password entry mistakes are made, thwarting intruders trying to guess your password.		🖱	🖱		
FILE/FOLDER ENCRYPTION Scrambles the language within your files while they sit unused on your hard drive. They automatically unscramble themselves when you log in.		🖱	🖱 XP Pro only	👍	
SECURE DELETE Writes garbled text over deleted files so your garbage is secured from intruders.				👍	
CD BOOT-UP PASSWORD Prevents potential intruders by requiring a password upon cd-boot up.					
DEFAULT IN/OUTBOUND FIREWALL Blocks security threats from coming in or going out of your computer.			👍 incoming traffic only	🖱	👍
CLOSED HIGH-RISK PROGRAMS Keeps high-risk programs (e.g.,FTP or Telnet) closed until you choose to open them.				👍	
CLOSED HIGH-RISK PORTS Ensures that only the minimum number of ports necessary for your network activities are left open, minimizing invasion of open vulnerable ports.				👍 if firewall is enabled	👍
DISABLE FILE-SHARING Allows file-sharing only within the applications you are actively using or wishing to share.		👍	🖱 XP Pro only		

* Based on the most recent, updated, patched versions of the operating system.
Questions about your operating system? Call IT Express: 754-HELP

👍 = included as default setting in OS
🖱 = user must enable feature in OS settings

Why Spam May Never Go Away

We all receive it and delete it, and most of us filter it. But spam still returns. Defined as unsolicited commercial email (from legitimate or illegitimate sources), spam used to be recognizable by its suspicious subject lines and unknown sender name. But now you can open an email that appears to be from your mother and find a shady business request from a foreign country instead. Perhaps the most troubling spam messages of late are the ones with strange combinations of nonsensical words followed by a URL (as if these incomprehensible messages would actually compel us to click on the link!).

Why Do They Do It and Why Can't We Catch Them?

Wading through all this, one wonders just who the spammers are and why they persist in believing we'll fall for their ridiculous and unappealing solicitations. According to Federal Trade Commission chair Tim Muris, most spammers do not represent legitimate businesses. They pelt thousands of email accounts with business pitches because it costs them very little to send. Even with an "extraordinarily low" response, they can turn a profit from those few takers. Furthermore, sending spam is low-risk because the anonymity of the Internet makes it difficult to catch the perpetrators. The only way to track them down, says Muris, is to follow the money trail from the consumer to the seller and back to the spammer.

Spam Gets Smarter

Unfortunately, there is no single solution to stopping spam, though there are ways to minimize it. For example, of the 17 million emails processed by UC Davis during January, 2004, nearly 6 million were tagged as spam and either automatically sent to a spam folder or automatically deleted. So why do those invasive email messages persist, regardless of successful filtering measures?

Since most spam filtering mechanisms are wired to recognize only the types of spam that they have filtered before, spammers create new variations of spam messages that can slip through the cracks in existing filters. Thus, there is often a window of time during which new spam is not yet recognized by filters and inboxes are flooded with a new iteration of the same old stuff.

Will CAN-SPAM Actually Can Spam?

State and federal lawmakers have recently begun to step up legislation efforts to stop the deluge of spam. The federal CAN–SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing) took effect at the beginning of 2004 and prohibits the use of commercial email to commit fraudulent or misleading acts. CAN–SPAM does not outlaw spam, but takes a stab at defining it, and delineating the wrong and right ways to serve up spam. CAN–SPAM requires that spammers provide a special subject line heading for messages containing sexually oriented material in addition to a functional "opt–out" option for recipients, allowing them to be taken off the spammer's mailing list, preventing future spam messages from the sender. Spam recipients have up to 30 days to utilize the opt–out function.

After CAN–SPAM was passed, the UC Office of the President deemed that all email from campus electronic mailing lists– to which people willingly subscribe– falls under the federal definition of spam. As such, much university email must now include a valid physical postal address of the sender and a clear means by which recipients can choose to opt out of receiving similar messages in the future.

For additional information about the CAN–SPAM Act or to read the UCOP guidelines for complying with the Act, visit security.ucdavis.edu/can_spam.cfm. ⚠

Safety First

TIPS FOR DEALING WITH SPAM

- **DO set up spam filtering at security.ucdavis.edu/spam.cfm.**
- **DO set up spam filtering for lists if you are a list owner at security.ucdavis.edu/spam_listowner.cfm.**
- **DO use filtering provided by your email program.**
- **DON'T open any document attached to a spam message as it very likely could be infected with a virus.**
- **DON'T ever reveal personal information via email. Legitimate businesses won't ask for account numbers, SSNs, or pin numbers over email.**
- **DO check your spam folder for legitimate email messages that may have been incorrectly identified as spam.**
- **DO send a complaint about received spam to the postmaster at the sending site; copy your complaint to ucdabuse@ucdavis.edu.**
- **DO use good judgment when choosing to reply to spam messages, even if just for an opt-out. Some spammers will interpret your response as an open invitation to send you more spam.**

●●●●●●●●●●●●TECHNEWS
http://technews.ucdavis.edu

IT Times is a companion publication to TechNews, a regularly updated news site providing technology headlines from UC Davis publications and other off-campus news sources. Visit technews.ucdavis.edu to read the latest headlines or to subscribe to the weekly TechNews email list that delivers the headlines right to your inbox.

The IT Times is published by the Office of the Vice Provost–Information and Educational Technology, University of California, Davis, to inform the campus community of information and educational technology services, initiatives, and activities at UC Davis. All content and design is produced by IET staff, unless otherwise noted. IT Times is distributed free of charge to members of the user community and to other universities. Use of trade or corporation names in this publication does not constitute endorsement by the University of California, Davis. IT Times articles may be reprinted as long as the source is accurately quoted and credited.

We welcome your input.
Contact: ietpubs@ucdavis.edu
Editor: E. Cayce Dumont (530)757-5796
Artist: Jeff Lagasca