SPECIAL EDITION

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 unwarded 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
bought online, the safest place to store that information
is on a computer. For this reason, we hope you’ll fi nd
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.

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 unwarded 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 bought online, the safest place to store that information is on a computer. 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.

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 unwarded 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 bought online, the safest place to store that information is on a computer. 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.
VIRUSES AND WORMS

What is it? Malicious small programs that easily replicate themselves, infect your computer, and often spread to other 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 pop-up advertisements that allow 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 “UD Resources” tab.

• Pick up “patches” at your operating system’s Web site to keep your computer fortified against possible attack.

• Reduce the 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 filenames, 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 or email attachments, infected disks, freeware, or file-sharing.

What is UC Davis doing to protect me?

• UC Davis is monitoring software and services that send an incoming and outgoing email to ucdavis.edu 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.

INSTANT MESSAGING

What is it? Instant messaging is popular because it is so convenient and because IMs, when used correctly, can be very secure. However, because IMs can be used to transmit viruses and files, they pose a security risk.

What risks are involved? Viruses can be very easily transmitted via instant messaging and are not encrypted, there is always a 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.

CONFIDENTIAL 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, 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) to 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 “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.

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 virus, or an 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 UCD’s Electronic Communications Policy, which details appropriate use of university email and the Internet. See www.ucdavis.edu/about/ucd/ethics/electroniccomms.

• 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.

• 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.

SHOPIING 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 measures (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 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.
WIRELESS NETWORK

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

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?
•  Refrain from online shopping to wired connections or to encrypted web browsers.
•  Use 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.
•  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.

FILES AND VIRUSES

What can I do to protect myself?
•  Re-read the UC Davis Internet安全 policy and Procedures document. In addition to this document, a section of the Security site is dedicated to fireswalls (security.ucdavis.edu/fireswalls.cfm), providing general information about fireswalls and links to additional resources.

FILE SHARING

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. 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 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 vulnerable programs.
•  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.

EMAIL ATTACHMENTS

WHAT THE CAMPUS IS DOING ABOUT COMPUTER SECURITY

DEPARTMENT FIREWALLS

In February 2004, a new and updated Departmental Firewalls 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 fireswalls (security.ucdavis.edu/fireswalls.cfm), providing general information about fireswalls and links to additional resources.

FILE ENCRYPTION

In response to new federal and state laws protecting personal information, a subgroup 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 and 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/identity.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/security/ spamfilter.cfm 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.

IDENTITY THEFT PREVENTION

With the passage of California Civil Code Section 1798 and 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/identity.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/security/ spamfilter.cfm 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.
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 can be 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!).

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 rightful ways to serve spam. CAN-SPAM requires that spammers provide a 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 after the date of the 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 of the sending site: copy a complaint to uddathuse@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.

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 of the sending site: copy a complaint to uddathuse@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.

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 can be 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!).

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 rightful ways to serve spam. CAN-SPAM requires that spammers provide a 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 after the date of the 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 of the sending site: copy a complaint to uddathuse@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.

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 of the sending site: copy a complaint to uddathuse@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.