
Information Security: It's Up To You

Get Informed, Get Involved

SYRACUSE UNIVERSITY



ITS

Information Technology
and Services





Information Security

Protecting University Information: It's Up to You

Syracuse University employees are exposed to all kinds of information in many different formats—student and employee personal records, financial and payroll information, Social Security numbers, SU I.D. numbers, and research data, to name a few. It is critical that all SU faculty and staff understand how to protect University information when they access or share this information using any kind of device—including desktop or laptop computers, hand-held devices, smart phones, and thumb drives—while working in their office, at home, across the country, or across the globe.

The University's greatest defense against unauthorized or unlawful disclosure of confidential information comes from alert, informed faculty and staff members who understand and follow good security practices.

Critical Information: A Case for Extra Protection

Many different kinds of information are transmitted and shared across the University every day. Some types of information are extremely confidential and employees must take added measures to protect this information.

The state and federal government have special regulations for maintaining confidentiality of some kinds of information, including the following:

- Information covered by the Federal Educational Rights and Privacy Act (FERPA). Most student information is covered under FERPA regulations.
- All information covered under the federal Health Insurance Portability and Accountability Act (HIPAA). Student and employee health information is covered by HIPAA regulations.
- Certain personally identifiable information (PII), including Social Security, credit card, and bank account numbers, are covered by state disclosure laws. Disclosure of such information to unauthorized parties is forbidden.

Examples of University information that may not be covered under state or federal regulations, but which also require extra layers of protection, include the following:

- Employee personal information, including, but not limited to, performance reviews, disciplinary actions, and salary information.

- University budget and financial information, grants and endowment information, donor information, and contract information.

Rule of thumb for assessing the sensitivity of information: What would happen if the information you use as part of your job requirements was stolen, posted on a public web site, or appeared on the evening news?

Accessing University Information

NetID and password: The first layer of defense

Access to the systems that contain University information is often controlled through the NetID and password. It is essential that all SU employees protect their NetID and password by maintaining good password practices:

- Don't share your password with anyone.
- Create a strong password by following the recommendations on the Information Technology and Services (ITS) security web site.
- Change your password once a year or if you suspect it may be known to someone else.
- Don't use your NetID password for any non-SU service, such as online banking or online shopping services.
- Never use your NetID and password to log onto open Internet services at web cafes or other public machines or wireless hotspots. These devices and networks are extremely insecure.

More information about good password practices is available on the ITS security web site at its.syr.edu/security/passwords.

Protecting your work station: The second layer of defense

It is critical that SU employee workstations be kept as secure as possible. Departmental computing support personnel are responsible for ensuring all University-owned computers are equipped with the University's recommended antivirus software and are updated with the latest operating system security patches, and for maintaining other security measures to prevent the computer from being compromised.

Employees are also responsible for ensuring their computer devices are secure by doing the following:

- Never download recreational software such as P2P file sharing programs, Weatherbug, or other free downloads from the Internet to any computing

device you use for work-related activities. These programs often include viruses, worms, Trojans, or other malware that compromise the security of your device and the confidential information you access with the device.

- Always log out of information systems when you leave your workstation, including e-mail, MySlice applications, MyReports, and Blackboard, or use a locking screen saver when you are away from your workstation.

- Lock your office door when you are away from your desk.

- Never leave a portable computing device unattended. Lock up all removable media.

- Web browsers are frequently targeted by hackers. Use caution when surfing web sites. Never allow your web browser to automatically install something from a web site. Beware of pop-ups and requests to install "ActiveX" on your computer.



Remote Access to University Information

The safest place for University information is on secure servers located on the University campus. However, many SU employees need to access University information from home or while away from campus for business reasons. It is critical that employees maintain the security of this information even when they are not on campus. SU provides specific tools and methods to allow secure access to University information and systems from remote locations. Details about how to gain remote access are available on the ITS security web site at its.syr.edu/security/remoteaccess/index.cfm.

Security tools: Ways to protect information you access when off campus

Virtual Private Network (VPN): The University's VPN system provides a secure network path between your remote computing device and the University's network, which helps protect the information exchanged across the Internet from eavesdroppers. Further information about the University's VPN service can be found on the ITS security web site at its.syr.edu/security.

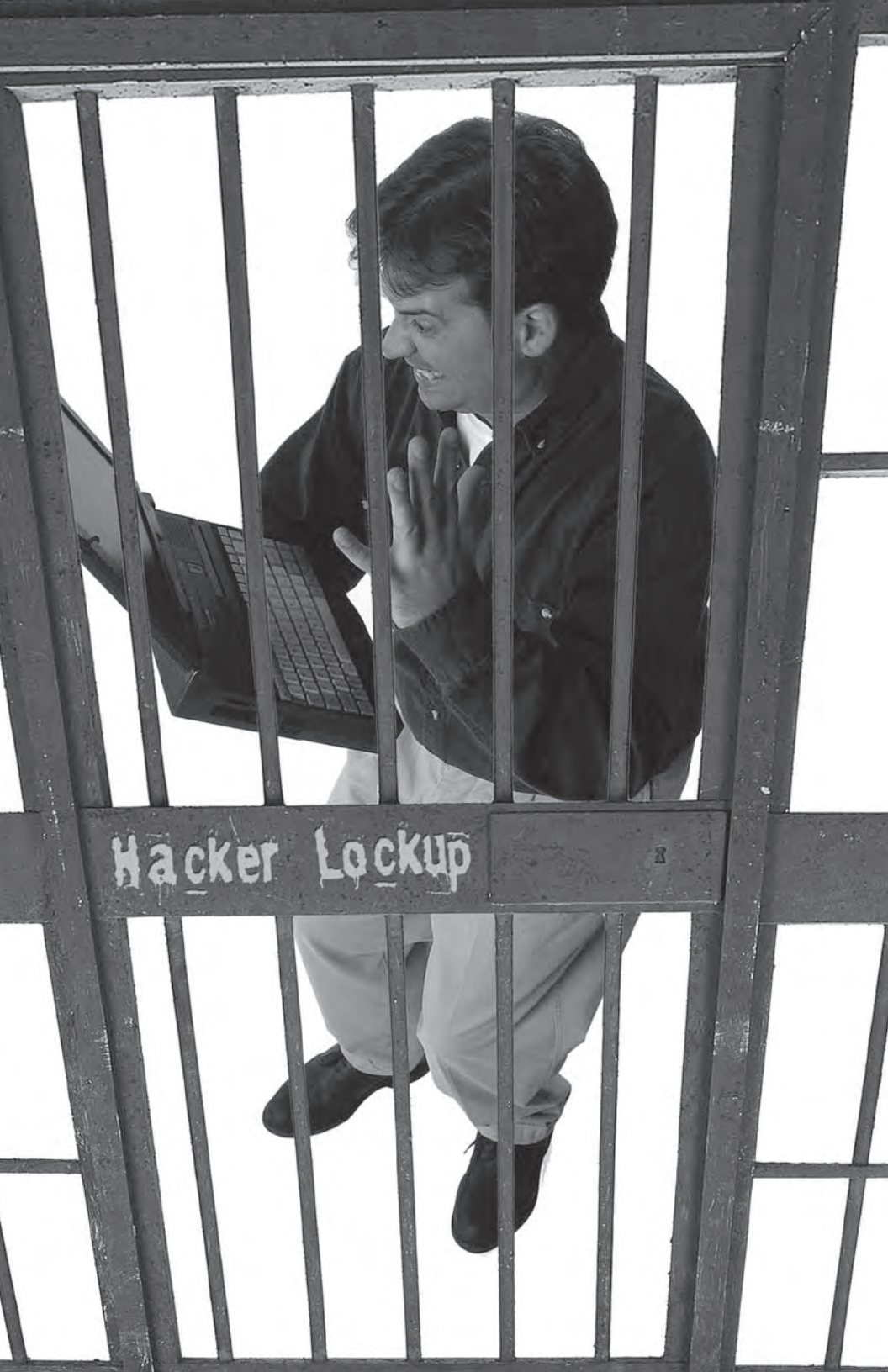
Remote Desktop: This tool enables employees to access data stored on their office computer from off-campus locations. It operates as if you were sitting at your office computer, so the data stays on campus. When used in combination with the VPN service, this tool gives employees access to important information from off-campus locations, while maintaining the security of that information.

Terminal Server: Some University departments store confidential data on a secure server, which employees can access via their NetID and password from on or off campus. These terminal servers work much like a remote desktop connection to your office computer, but are used by more than one person. Information stored on these servers cannot be downloaded onto insecure computing devices, such as laptop computers or thumb drives.

Transmitting and Sharing University Information

It is sometimes necessary for University employees to share or transmit information to colleagues or outside vendors.

- Share University information only with authorized individuals who require access as part of their University role or with external parties who have been approved by the owner of the information or by your department or unit.
 - Use only those methods recommended by your departmental computing support person for sharing confidential information.
 - Never copy confidential information onto an unsecured personal laptop computer, home computer, thumb drive, CD, or other removable media device.
- About e-mail:** Confidential information is frequently transmitted via e-mail. Faculty and staff must be extremely cautious when using e-mail for this purpose. In many cases, e-mail traffic flows over insecure networks, particularly when senders are communicating with someone outside of



Hacker Lockup

the University's e-mail system. Therefore, sensitive information should not be sent via e-mail unless the sender and receiver use the same campus e-mail system (e.g. Information can be safely shared if both parties use the University's Outlook/Exchange system or if both parties use GroupWise). When in doubt, ask your local computing support person or e-mail itsecurity@listserv.syr.edu.

Instant messaging, chat programs: These kinds of commercial communications systems send information through external servers that are not part of the SU network infrastructure and are not controlled by SU. In many cases, the information is not protected while it travels over the Internet. Therefore, never use these methods for exchanging sensitive information.

The Final Key: Foiling Hackers and Thieves

SU employees are the key to protecting the University's information resources. Here are some simple things you can do to help keep SU information resources out of the hands of hackers and thieves.

- **E-mail pitfalls:** Always be wary of unsolicited e-mails. Do not open e-mail attachments unless you are expecting an attachment from a friend or colleague. Never click on links embedded in unsolicited e-mails. Beware of phishing scams and other Internet hoaxes that attempt to trick you into revealing your personal information, such as bank account, credit card, and Social Security numbers or account passwords.

- **Phone calls:** Always be wary of unsolicited phone calls from people looking for any kind of employee or student information or access to accounts.

- **Information-security shortcuts:** Always be wary when someone asks you to violate common, information-security practices or take security "shortcuts."

- **When in doubt:** Call your supervisor; call the ITS Help Desk at 315-443-2677; or e-mail itsecurity@listserv.syr.edu.

Get Informed, Get Involved

More information about SU security policies, procedures, and safe computing is available on the ITS Security web site at its.syr.edu/security.

