Information Technology Security Awareness

Computer crimes are on the rise and damage being done by them is becoming more severe. Large servers, desktop computers, laptops, printers, hand-held PDA's, and other devices are all targets for foul play. The good news is that every computer user can take steps to reduce the likelihood of being a victim, and, as a member of the U.Va. community, every computer user has the responsibility to do so.

The purpose of this security awareness tool is to explain the most critical threats to our computing environment and the actions individuals must take to safeguard against those threats. It also covers what is considered responsible use of University computing resources, including careful protection of confidential University data.

At the end of the training session you will be asked to acknowledge your agreement to abide by University computing policies and applicable laws, which are summarized in the Responsible Computing Handbook. If you access Medical Center computer systems, additional security policies apply. You may wish to read this information before starting the training.

Please click below to begin the training process, which will take between fifteen and twenty minutes to complete.
Are Universities Really Targets?

Few people haven't heard about at least one major computer attack; widespread computer attacks and identity theft are regularly reported in the news. Recent estimates are that organizations worldwide are losing billions of dollars annually due to computer security breaches. Not only can quantifiable assets be lost due to attacks, but a company's customer service can also be compromised, its reputation tarnished, and its risk of litigation increased. Identity theft is also on the rise.

Universities are hardly immune to such attacks. In fact, they have become favorite targets for cyber criminals. In the past few years, all of the following incidents have occurred at major universities:

- Confidential student, employee, donor and medical data have been stolen.
- University computers have been used to launch attacks on businesses and the Federal government.
- Research data have been compromised.
- Networks and mail systems have been rendered useless for days.
- University computers have been confiscated by FBI investigators.
How Might You Be Personally Affected?

Your emails and other confidential data could be exposed or lost.

Your user ID and password could be stolen and then used to wreak havoc on other computers (in your name).

Sensitive University data that you have the responsibility to protect could be stolen or inappropriately altered.

You could lose access to the University's network and the Internet while a security breach is being investigated.

Keep in mind that computer attacks are crimes, and people can easily become unwilling accomplices just as they can be with other crimes. If your computer is used by someone else to commit a crime, you could find the FBI knocking on your door the next day. It happens, and it is serious business.
Can You Really Make a Difference?

To fully understand the dangers out there in the Internet world, it's important to dispel the myth that successful computer attacks are the deeds of brilliant masterminds. The truth is most attackers are just average Joe and Josephine Blows with mischief on their minds. Information about the vulnerabilities of all types of devices is widely available on the Internet, as are instructions and software tools for launching attacks.

Many successful attackers today simply take the easy road; they exploit well-known vulnerabilities with tools handed to them on a silver platter. By taking a few simple steps, security-aware computer users can foil these attempts. These steps are explained on the following pages.

All University computer users should understand the basic security issues discussed in this training. It is valuable knowledge for securing both work and home computers. In certain departments, however, some of the specific instructions may be the responsibility of local computer support personnel rather than the individual user. For example, some local computer support personnel manage anti-virus and other software updates for all computers in their departments.
Use Up-To-Date Anti-Virus Software

Computer viruses can lock up your computer and destroy data stored there within seconds of spreading to your computer; however, anti-virus software is available free to U.Va. employees and students and does an excellent job of inoculating your computer against known viruses. If you don't have this software, get it and install it now. Be sure the software runs continuously on your computer, allowing it to constantly protect against attack.

Also, just as flu vaccines must be annually adjusted to address new strains of the flu virus, anti-virus software should be updated daily to make it "aware" of new virus types. Additional information on anti-virus software is provided at the end of this training.
Correct Software Defects

Software is no different from any other product - flaws can show up long after it has been produced. Most car owners, for example, have at one time or another been sent a manufacturer recall notice to address a quality defect. Software products have defects, too. Unlike cars, however, software is never recalled and fixed by the developer. Instead, the developer publicizes software "patches" that, when applied, will correct defects.

Software owners are expected to discover the availability of these patches on their own and apply them themselves. When software patches designed to correct security-related flaws are not applied, the computer running that software remains vulnerable.

Most of the vulnerabilities discovered over the past few years have been in computer operating system software, like Windows. Fortunately, the most recent operating system versions allow the patching process to be automated. Also, a free service to keep your Windows system updated is available to U.Va. employees. Additional information about this service is provided at the end of this training session.

Web browsers, word processors, and other application software present similar risks. Unless a computer support person is assigned the responsibility to keep all software on your computer up to date, at least monthly check the web sites of the software vendors you use to learn about the availability of new software patches. If the vendor offers an email notification service for software patches, sign up for it. Always download patches that correct security-related defects for your software version. Instructions for downloading and applying patches are provided on these sites.
Clean Up and Lock Down

Turn off or delete unneeded software features - The more software products you have on your machine, the more opportunity there is for exposure. Products that are not used should be removed. Also, products often include features that can be turned off or on. Computer users should read the software manuals, paying particular attention to such features. Unneeded features should be turned off.

Turn off file sharing - The file sharing capability of your computer should be enabled only if it is essential that others be able to access files on that computer. Also, make sure your machine is physically secured to prevent tampering.

Enable your operating system firewall - A firewall is an application that can prevent other computers from making unsolicited connections to your machine. It can offer critical protection against attacks. Windows XP and Mac OSX operating systems have a built-in firewall, but it's important to verify it is turned on.

Further guidance on these safeguards is provided at the end of this training session.
Know Whom You're Dealing With

You wouldn't fling your front door open without first checking who's there, right? Be equally cautious about downloading free software or other files from the Internet and opening attachments to emails. Each time you encounter a new file, judge carefully the reliability of the file's source and contents before you open it or save it to your computer. It's best never to open an attachment unless you are absolutely sure of the credibility of both the sender and the contents of the sent material.

Also, if someone walks up to you on the street, says she's a teller from your bank, and asks for your bank account number, you wouldn't give it to her, right? React the same way to unsolicited email messages that request your personal information, such as social security number, credit card number, and password, even if the request appears to be from a bank or other company with which you do business. Legitimate organizations don't ask for personal information unless you go to them to open an account, purchase a product or service, or conduct other business.
Use Strong Password Protection

Some types of computer attacks aren't possible if the attacker can't guess your computer logon password. Unfortunately, they have tools available to them that are awfully good at guessing passwords. Learn what constitutes a good password (see tips below) and memorize, rather than write down, the ones you create. Don't share your passwords with others, and change them if you know or suspect they have been revealed to someone. A strong password has these characteristics:

- It consists of eight or more characters.
- It uses both upper (A-Z) and lower-case (a-z) letters.
- It includes one or more numbers (0-9).
- It includes one or more special characters, such as a question mark or an asterisk.
- It does not contain a name or a word found in the dictionary.

It's important for a password to be easy to remember so you won't be tempted to write it down. As a suggestion, think of a sentence you'll remember, use the first letter of each word in the sentence, and then throw in a digit and/or special character somewhere in the middle. For example:

- Lunch usually costs me $10 or less (Lucm$10ol)
- It Takes Two is my favorite song (IT2!imfs)
- Where shall I go on vacation this year (w?s1goVty)
Back Up, Back Up, Back Up

Because successful attacks often harm data on your computer, fully recovering from them often requires your data files to be overwritten from a backup copy. If you haven't recently saved your data to a CD or other storage medium, that data will be lost forever. Be sure at least your critical data files are backed up whenever they are updated and backups are kept where they will be available in the event of an emergency, but in a different physical location than the original files.
Fully Protect University Data

The information of any organization is one of its most valuable assets. Now that University of Virginia business is conducted extensively on computers and the information is available more readily and to greater numbers of persons, you have an important responsibility to protect it. Adhering to the safeguards just covered will help you meet that responsibility. In addition,

- Log off your computer when you leave your desk and use a password-protected screen saver. Keep information displayed on your screen confidential, just as you would keep confidential printed material on your desk or in your files away from wandering glances.
- Reformat used diskettes and rewritable CDs and use them again. Destroy diskettes, CDs, and other electronic media when they are no longer reusable. Do not recycle any that contain sensitive data or University-licensed software.
- Lock your diskettes, CDs, and other electronic media in your desk or in a locked, fire-resistant cabinet.
- Follow University-approved procedures when surplusing electronic devices such as desktop computers, laptops, and PDAs, returning them to a leasing company, or transferring them from one University employee to another employee having different software and data access privileges.
- It is not advisable to use E-mail for confidential information or when there would be concern if all or part of the E-mail were forwarded to other parties.
- Use of a mobile device, such as PDA, Blackberry, or text-enabled pager, for sending and receiving messages containing confidential information is especially discouraged, because a mobile device can be easily lost or stolen. All messages containing confidential University information should be promptly deleted.
- Apply the security safeguards discussed in this training not just to on-site devices and data, but also to protect devices and data taken off University premises. Special precautions are necessary for small portable devices (such as laptops and PDAs), which can be easily lost or stolen. Home computers used for University business should be secured.
- If you become aware that sensitive University data may have been inappropriately exposed, contact the ITC Security and Policy Office at itc-security@virginia.edu.
- Your electronic data files are extensions of printed files in your care. It is your responsibility to ensure that both electronic and paper files in your care be safeguarded, especially if they contain sensitive information such as data about individual students, employees, patients, research participants, donors, and others. If you are unsure what is expected of you, ask questions.
Know And Follow Data Privacy And Security Regulations

There are University policies, and State and Federal regulations, governing the privacy and security of data. Personal information about students, employees, patients, research participants, donors, and other individuals is especially of concern. It must not be accessed unless you need to do so as part of your responsibilities, or disclosed except in accord with these policies and regulations. Read and understand these policies and regulations and take time to see how they apply to your responsibilities. If you use Medical Center information systems, or patient information, read and understand Medical Center policies as well. Ask questions if you are unsure of what is expected of you.

A list of key policies and regulations is provided at the end of this training session. Be aware that if you violate University or Medical Center policies on data privacy and security, you can be subject to disciplinary action including, for serious violations, suspension or even termination of your employment.
Be A Good Internet Citizen

The University provides Internet access to faculty, staff, and students with the expectation that they be good, responsible, and accountable Internet citizens. But, what does that mean in practical terms? How can you be a good Internet citizen?

- **DON'T** let colleagues, relatives, or any other person gain access to the University's computing resources through your account. Understand that you will be held accountable for any abuse of computing resources by persons who use your U.Va. computing ID and password.
- **DON'T** use computer accounts, computing IDs, and passwords that belong to someone else. To do so violates policy.
- **BE ACCOUNTABLE** for your actions. Hiding your identity to avoid responsibility for your behavior on the network or using someone else's network identity are - at a minimum - violations of policy, and they may be serious violations of law.
- **DON'T** engage in online activities that waste shared computing resources and have no mission-related purpose. You are not authorized to use your computing account or access to do so.
- **KNOW** that local, state, and federal laws and regulations pertain to computing activities wherever appropriate - laws dealing with fraud, forgery, harassment, extortion, gambling, threats, copyright, obscene content, and misuse of confidential data such as data regarding students, employees, patients, research participants, and donors, among others. Violators may be prosecuted, and face disciplinary action as well.
- **BE WARY** of those who will (sometimes unknowingly) provide online information that is untrue or fraudulent. If you are not certain, ask.
- **KNOW** that messages you post to newsgroups or Web pages in an attempt to be humorous may not be received in that spirit. Remember that archives of newsgroups and Web pages remain accessible for years.
- **DON'T MISUNDERSTAND.** Your access to computing resources can be revoked. In extending these resources, the University trusts faculty, staff, and students to make responsible use of them. If you violate that trust, you may lose access.
To reinforce what you have just read, you will now be asked a few questions.

**This is question 1 of 8. Please choose the answer that is most correct.**

- What steps must I take to prevent someone from breaking into my computer?

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Use up-to-date anti-virus software</td>
</tr>
<tr>
<td>B</td>
<td>Correct software defects</td>
</tr>
<tr>
<td>C</td>
<td>Turn off or delete unneeded software features</td>
</tr>
<tr>
<td>D</td>
<td>Turn off file sharing</td>
</tr>
<tr>
<td>E</td>
<td>Use a firewall</td>
</tr>
<tr>
<td>F</td>
<td>Use strong password protection</td>
</tr>
<tr>
<td>G</td>
<td>All of the above</td>
</tr>
<tr>
<td>H</td>
<td>A, B, and F</td>
</tr>
<tr>
<td>I</td>
<td>A and F</td>
</tr>
</tbody>
</table>

Continue
Correct!
You answered the previous question correctly. To review:

Because someone can break into your computer in a number of different ways, multiple defenses are necessary to prevent attack. Taking just one step is not enough. All advice provided in this training session should be heeded. Links to additional tips and information on protecting your computer are provided at the end of the session.
Problem:
What steps must I take to prevent someone from breaking into my computer?

Issues:
Because someone can break into your computer in a number of different ways, multiple defenses are necessary to prevent attack. Taking just one step is not enough. All advice provided in this training session should be heeded. Links to additional tips and information on protecting your computer are provided at the end of the session.
This is question 2 of 8. Please choose the answer that is most correct.

- Why should I care if someone breaks into my computer?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(A) My emails and other data could be read or deleted.</td>
</tr>
<tr>
<td></td>
<td>(B) My user ID and password could be stolen and then used to attack other computers (in my name).</td>
</tr>
<tr>
<td></td>
<td>(C) Sensitive University data for which I am responsible could be stolen or altered.</td>
</tr>
<tr>
<td></td>
<td>(D) My computer could be disconnected from the University’s network while the attack is under investigation.</td>
</tr>
<tr>
<td></td>
<td>(E) All of the above</td>
</tr>
<tr>
<td></td>
<td>(F) A, B, and C</td>
</tr>
</tbody>
</table>
A successful attack on your computer could have very serious consequences. For example,

- Your emails and other confidential data could be exposed or lost.
- Your user ID and password could be stolen and then used to wreak havoc on other computers (in your name).
- Sensitive university data for which you have the responsibility to protect could be stolen or inappropriately altered.
- You could lose access to the University's network and the Internet while a security breach is being investigated.

Keep in mind that computer attacks are crimes, and people can easily become unwilling accomplices by not adequately protected their computers. If your computer is used by someone else to commit a crime, you could find the FBI knocking on your door the next day.
When is it safe to assume that a brand-new computer is free of security vulnerabilities?

- Always
- Never
- Only when it is purchased from a reputable company
Correct!
You answered the previous question correctly. To review:

Never assume a new computer is free of security vulnerabilities, even if it is purchased from a reputable company. The software on a new computer may not, for example, include the latest updates that correct security-related software flaws, and anti-virus software may not be installed on the computer. The steps described in this training session to protect your computer from harm are equally important for new computers as they are for older computers.
This is question 4 of 8. Please choose the answer that is most correct.

- What type of software must be kept updated with security software patches?

- All operating system (an example is Windows) and application software (an example is Word)
- Only operating system software
- Only application software
Correct!
You answered the previous question correctly. To review:

Most software vulnerabilities discovered over the past few years have been in computer operating systems; however, web browsers, word processors, and other application software present similar risks. When software patches designed to correct security-related flaws are not applied, the computer running that software remains vulnerable to attack.
This is question 5 of 8. Please choose the answer that is most correct.

- Which of the following actions can be risky?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>Opening an email attachment from a friend</td>
</tr>
<tr>
<td>☑</td>
<td>Downloading free software from the Internet</td>
</tr>
<tr>
<td></td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>Neither</td>
</tr>
</tbody>
</table>

Continue
Correct!
You answered the previous question correctly. To review:

Cyber criminals use several methods to trick computer users into loading malicious software onto their computers, including disguising themselves as someone else. Be cautious about downloading free software or other files from the Internet and opening attachments to emails. Each time you encounter a new file, judge carefully the reliability of the file’s source and contents before you open it or save it to your computer. It’s best never to open an attachment unless you are absolutely sure of the credibility of BOTH the sender and the contents of the sent material.
This is question 6 of 8. Please choose the answer that is most correct.

- Which of the following is the strongest password?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>John</td>
</tr>
<tr>
<td>☐</td>
<td>Administrator</td>
</tr>
<tr>
<td>☐</td>
<td>FortKnox</td>
</tr>
<tr>
<td>☐</td>
<td>Secret</td>
</tr>
<tr>
<td>☑</td>
<td>w?sgovty</td>
</tr>
</tbody>
</table>
Correct!
You answered the previous question correctly. To review:

A strong password has these characteristics:

- It consists of eight or more characters.
- It uses both upper (A-Z) and lower-case (a-z) letters.
- It includes one or more numbers (0-9).
- It includes one or more special characters, such as !@#$%^&*()_+-.
- It does not contain a name or a word found in the dictionary.
You have received an email message saying that your credit card is over the spending limit. The message instructs you to click on the provided Internet address in the email and enter your name, address, and credit card number in order to check your balance. What should be your next action?

- Click on the provided Internet address and enter your name, address, and credit card number
- Delete the message
- Forward the email to your friends so they can check their credit card balances
Correct!
You answered the previous question correctly. To review:

React very cautiously to unsolicited email messages that request your personal information, such as social security number, credit card number, and password, even if the request appears to be from a bank or other company with which you do business. Legitimate organizations don’t ask for personal information unless you go to them to open an account, purchase a product or service, or conduct other business.
This is question 8 of 8. Please choose the answer that is most correct.

- Which one of the following statements is false?

<table>
<thead>
<tr>
<th>Option</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>My access to computing resources can be revoked if I fail to use it responsibly.</td>
</tr>
<tr>
<td>☐</td>
<td>The University holds me accountable for keeping my computer free of vulnerabilities.</td>
</tr>
<tr>
<td>☐</td>
<td>The University holds me accountable for protecting University data, especially data about individual students, employees, patients, research participants, donors, and others. I must not access this data unless I need to for my work, or disclose it unless allowed by applicable policies and regulations.</td>
</tr>
<tr>
<td>☐</td>
<td>If someone steals my user ID and password, I’m not responsible for what he or she does with it.</td>
</tr>
</tbody>
</table>
Correct!
You answered the previous question correctly. To review:

In support of its mission of teaching, research, and public service, the University of Virginia provides faculty, staff and students with access to computing and information resources. Responsible behavior is the price of admission to the University’s digital community, with its attendant conveniences and benefits. Irresponsible behavior can jeopardize your computing privileges and can put you at risk for other serious consequences. You are accountable for abuse of computing resources by persons who use your U.Va. computing ID and password, so guard these carefully.
If any of the refresher questions were answered incorrectly, they are re-asked here. The employee is unable proceed to the next screen until all questions are correctly answered.
ACKNOWLEDGEMENT OF RESPONSIBILITY

In support of its mission of teaching, research, and public service, the University of Virginia provides employees access to computing and information resources. Use of these resources is governed not only by the University's own policies, but also by local, state, and federal laws relating to copyrights, privacy and confidentiality, security, and other statutes regarding electronic media.

A summary of these regulations are provided in the <> . Failure to follow these policies and laws may result in the revocation of your computing privileges and/or other disciplinary actions, including termination of employment.

Please acknowledge below that you will abide by University computing policies and applicable laws.

[ ] I will abide by University computing polices and applicable laws.

[ ] I will NOT abide by University computing policies and applicable laws.
If the employee answers “I will abide by…” to the Acknowledgement of Responsibility question, he/she is taken to the Certificate of Completion page. Otherwise, he/she will be given one more chance to response correctly. If the employee still does not acknowledge responsibility, he/she is instructed to read the Responsible Computing Handbook and retake the training and will remain on the list of employees who have not yet completed training. The next few pages show the text associated with this process.
You did not acknowledge that you would abide by University computing policies and applicable laws, an essential step to successfully complete this training.

If you wish to change your answer, please do so below. Otherwise, read the Responsible Computing Handbook (and Medical Center security policies if you access Medical Center computer systems) and retake this security awareness training at another time.

- **ACKNOWLEDGEMENT OF RESPONSIBILITY**

  In support of its mission of teaching, research, and public service, the University of Virginia provides employees access to computing and information resources. Use of these resources is governed not only by the University's own policies, but also by local, state, and federal laws relating to copyrights, privacy and confidentiality, security, and other statutes regarding electronic media.

  A summary of these regulations are provided in the Responsible Computing Handbook. If you access Medical Center computer systems, additional security policies apply. Failure to follow these policies and laws may result in the revocation of your computing privileges and/or other disciplinary actions, including termination of employment.

  Please acknowledge below that you will abide by University computing policies and applicable laws.

<table>
<thead>
<tr>
<th></th>
<th>I will abide by University computing policies and applicable laws.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I will NOT abide by University computing policies and applicable laws.</td>
</tr>
</tbody>
</table>

Continue
You did not acknowledge that you would abide by University computing policies and applicable laws, an essential step to successfully complete this training. University computer users are required to follow them. Failure to do so could result in:

- revocation of your computing account,
- disciplinary action, and/or
- possibly even criminal prosecution in the event laws are broken.

Read the Responsible Computing Handbook (and Medical Center security policies if you access Medical Center computer systems) and retake this security awareness training at another time.
CERTIFICATE OF COMPLETION

John Doe has successfully completed the Information Technology Security Awareness training administered by the University of Virginia Information Technology & Communication Department.

Date of completion: 02/13/2006

Additional Reading

Links to more detailed information on computer security and responsible use are provided below.


Tips for correcting software defects, enabling firewalls, and other steps for securing your computer can be found at http://www.itc.virginia.edu/security/checklistforPCs.phtml


Learn about ITC’s Windows software update service at http://www.itc.virginia.edu/microsys/patchmanagement.html

A summary of University computing policies is provided at http://www.itc.virginia.edu/policy. All are important, but see in particular the:

- Responsible Computing Handbook for Faculty and Staff http://www.itc.virginia.edu/pubs/docs/RespComp/resp-comp-facstf.html
- Attaching Devices to the Network Policy http://www.itc.virginia.edu/policy/netdevices

The following are key laws regarding data privacy and security:

- The Family Educational Rights and Privacy Act, or FERPA, requires the University to protect the confidentiality of student educational records. These include academic records, financial records, disciplinary records, medical records and placement office records. See http://www.virginia.edu/registrar/privacy.html
- The Gramm-Leach-Bliley Act requires that personally identifiable financial data, such as bank and credit card account numbers, be safeguarded against unauthorized access or use. See http://www.nacubo.org/x2152.xml
• The Health Insurance Portability and Accountability Act requires that protected health information -- identifiable information about patients and research participants -- be safeguarded against unauthorized access or use. See http://www.cms.hhs.gov/hipaa

• Retention, protection and filing practices and techniques for all files and records is governed by the Commonwealth of Virginia Public Records Act. Where necessary the University will develop specific regulations and procedures for electronic media within departments needing standards for electronic file organization, measures for protecting sensitive information stored electronically, and procedures for file backup and restoration. See http://www.lva.lib.va.us/whatwedo/records/vpra.htm

The Medical Center Information Security website, which includes a list of Medical Center security policies, is available at https://www.healthsystem.virginia.edu/intranet/security

☐ Check here if you'd like this information emailed to you.

Continue
Thank You

Thank you for using this security awareness tool. If you have questions or comments, please email those to the ITC Security and Policy Office.