Security for Auxiliary Services Computers

In today's world computer security is a matter of utmost importance. Society has come to depend on the computer for many day to day functions, such as E-mail, web surfing, administrative tasks, and many other functions. When a computer has been compromised it may have an impact not only on the user, but on everyone associated with the user. By following the steps below you will be able to help keep your computer safe.

Passwords:

A password is one of the most important steps in keeping your computer secure. It allows only you to login to your account. If your password is simple or shared with others you have decreased your computers security. Anyone that has your password will be able to logon to the computer. In doing so, who knows what they are doing when they are on it. If a hacker can get past your password they not only have access to your computer, but to the other resources that you have access to.

A secure password is one that involves not only numbers and letters, but also characters such as !@#$. Passwords are also case-sensitive, which means that "password" does not mean "PaSsWoRd". A good password should be no less then eight characters. It should not include any words from the dictionary and should not be anything that identifies you personally, such as a pet's name. DO NOT USE YOUR NAME. Remember the password allows you to access not only your computer, but also the resources it's connected to. It is also a good idea to change your password if you tell it to someone or have used it for a few months.

Some simple rules of thumb

Some simple guidelines that will help you choose better passwords are:

- A password should be a minimum of eight characters long.
- Try to use a combination of numbers, letters, and punctuation marks.
- Use mixed case passwords if possible.
- Choose a phrase or a combination of words, that make the password easier to remember.
- Do not use a word that can be found in any dictionary (including foreign language dictionaries).
- Do not use a keyboard pattern such as qwertyui or oeuidhtn (look at a Dvorak keyboard).
- Do not repeat any character more than once in a row like zzzzzzzz.
- Do not use all punctuation, all digit or all alphabetic.
- Do not use things that can be easily determined such as:
    - Phone numbers.
    - Car registration.
    - Friends' or relatives' names.
    - Your name or employment details.
    - Any Date.
- Never use your account name as its password.
- Use different passwords for each machine.

Change the password regularly and do not reuse passwords.

Do not begin or end a word with a number or punctuation mark.

Do not reverse words.

Do not replace letters with similar looking numbers. For instance, all of the letters i should not be blindly replaced by the digit 1.

Examples of how to construct good passwords

So now that typical bad passwords have been discussed, how is a good password constructed? Try combining two or more words together or taking the first (or second or last) letter of each word in an easily remembered phrase. Then mangle the result by adding capitals, digits and punctuation characters. As an extra measure, control characters can also be introduced.

Some examples of using multiple words with punctuation

Here is a pair of good examples of using multiple words:

gOt%L0st! - got lost!

heLP4me$ - help for me (money)

And here is a bad one:

T0gether - to get her

Some examples of using a phrase

Here are three good examples of using phrases:

rsKf0myH - Raindrops keep falling on my head.

wru2rxy? - Who are you to ask why.

bWiIso3! - Beware the ides of March!

And here is a bad one:

Aaaaaaaa - Always assert an ambiguous axiom and argue aggressively.

As a final note, all the sample passwords listed in this article are now known, and should not be used by anyone.

You should not write down your passwords. If you feel that you will forget the passwords and do need to write them down, do not leave them near the computer. Place them someplace safe such as your wallet or purse.

There are different levels of passwords. Some have to be installed or enabled before you will be prompted to enter them. There are power-on passwords (BIOS passwords) that you are required when you turn on or restart the computer. There is also your windows logon password which is required to login to windows. Additionally you may need passwords for administrative programs such as Banner or QuickBooks. Each of these passwords should be different. Knowing one password should not let a person into everything you use.

Protecting your computer with a BIOS password allows only the person with the password to start or restart the computer. A second step is to set the BIOS so the computer can not be booted from any other device than the hard disk drive. Please contact the ResNet Helpdesk @1929 to arrange for help in securing your BIOS.

Your Windows password allows you to login to your user account. This allows access to your network shares/resources and any programs you use. It also allows access to any administrative programs such as Banner and CSGold. These programs also require usernames/passwords, however they should have especially protected passwords as they access confidential information such as student ID numbers.

Operating System Updates:

To ensure your computer is up to date, open Internet Explorer and choose "Windows Update" from the Tool menu. When the update site appears click express install. Windows updates will search for updates your computer needs. Once it has scanned your computer you will need to press the “Install Updates” button. Updates also help to stop the spread of viruses and hacking.

As a precaution, ResNet sets up all new computers (and many older systems) with AutoUpdates turned on. Your computer will automatically download the new updates and tell you that they are ready to install. If you notice a “balloon” pop-up next to the clock on the computer telling you new updates are ready to install, please take the time to install these immediately as it will save time in the long run.

Firewalls:

A firewall is a barrier between your computer and the rest of the Internet. Its purpose is to keep vulnerable ports closed to the rest of the world. An open port allows access to your computer that many viruses and hackers can take advantage of. Once a virus has infected your computer it may use the computer to spread from it. A virus might also open ports that make the computer accessible to the outside world and to a hacker just waiting to exploit the situation.

To enable the Windows firewall, click on the start menu and then on Control Panel (which might be located in the settings menu). Double click the “Windows Firewall” control panel and check to see that “on” is selected.

ResNet has deployed a hardware firewall to protect server functions. This is a basic security measure aimed at protecting the databases and server data from attack.

Viruses:

Make sure that your virus scanner is up-to-date and is set to update automatically. This can be done by clicking on the Start Menu, clicking on Programs, choosing the Network Associates Folder and choosing "VirusScan Console". Confirm "AutoUpdate" is set to "Daily" and the time is a time your computer will be on. If you need to adjust the time double click

"AutoUpdate" and choose schedule, then choose the schedule tab. Make sure that "Schedule Task" is set to daily and that the "Start Time" is a time your computer will be powered up. Click "OK" until you are back to the VirusScan console. Right click on "AutoUpdate" and choose "Start".

Once the virus scanner is updated, it is a good idea to run a virus scan every once in a while to keep your computer clean. While still in the Virusscan console right click "Scan All Fixed Disks" and choose start. Right before you head out to lunch would be a good time to run this process as it does use up local system resources.

Adware/Spyware:

Adware/Spyware are programs that are installed on a computer usually without your knowledge. These programs are often installed either as the "cool new program" you found and want to use, or they are installed with the program. Programs such as Hotbar, Precison Time, Weatherbug, and Webshots just to name a few are not only spyware, but they also slow down your computer and the network. These programs may not only use many of your system resources, causing your computer to become slow, but they may also cause malicious damage to your computer. In some cases they may even be able to steal data or track the things you do. Getting one of these programs is as easy as opening a web page that is designed to lure you into believing you need the program on your computer. There are programs designed to combat Adware/Spyware. A program loaded on your computer called Spybot Search and Destroy will help in the removal of these types of programs. Spybot also has the ability to immunize against spyware. Please contact the ResNet Helpdesk @1929 with any spyware questions.

File Shares:

Sharing documentation with your coworkers is great; however, you should not share the information directly from your computer. Using your computer to share files can open your system to many security risks, such as playing host to viruses. The best course of action is to use a secure file share area that has most likely been set up for your department already. Note that files stored on the servers should be work related. If you wish to share your photos of your Florida trip E-mail them to the person you wish to share them with.

File sharing programs also referred to P2P programs (Kazaa, Morpheus, Limewire, WinMX, just to name a few) should not be installed on any system. Sure free music, movies, programs sound great, but they are not free. When you use these programs not only are you stealing from someone that has put a lot of time and effort into their work, but you are also opening your computer up to possibly let them view your files. It can also allow a gateway to allow other people not affiliated with MSU to use valuable campus resources. Also many of the P2P programs include spyware/adware which may affect the performance of your computer. These programs may also lead to serious legal issues not only for you but for the university as well.

Software Licenses:

Most software is not free. Your computer should only have legitimate programs running on it. Software companies expend a lot of time and money to develop their programs. Just because you have the CD and a key does not mean you may use it on as many computers as you wish. When installing a program please ensure that you are staying within the original license agreement.

Social Engineering/Hackers:

Beware of anyone that would call and ask for your password. A question you need to ask yourself is, "Why do they need it?" If you are convinced that the person genuinely needs the password, let them know you will call them back. Get their name and department and verify against the staff directory the phone number for that person. This is also important when dealing with E-mail. Many spammers will send you information pretending to be with a real company to try and get your information from you. Say for instance you receive a notice from your bank saying they need your username and password. There is no reason whatsoever they should need this password. They have it in their system. E-mail addresses can be phony. If you receive any type of message for information, confirm that it is legitimate by calling a number you have on file.

A ploy used by scam artists is called “phishing”. It is the art of sending an E-mail that appears to come from a legitimate source such as your bank. Often times the E-mail will say something like “Your account information needs to be updated! Click here!” When you click the link it directs you to a site that someone has set up to capture your username and password and any other information you provide. The best way to avoid these situations is to call the institution requesting the information and verify with a representative the legitimacy of the E-mail. Most banks have a standard practice that they will not E-mail you for information.

Attachments:

Beware of attachments you receive. If you are not expecting an attachment DO NOT OPEN IT! Likewise if you use an Instant Messaging program do not accept attachments without verifying their authenticity. Even if you know the person sending the message, there is no guarantee that their computer has not been compromised and is sending infected attachments without their knowledge. Attachments can carry additional programs/virus’s that are unwanted. By opening an attachment, you are giving it permission to execute the code and infect the machine.

Physical security:

Every time you leave your desk you are leaving your system vulnerable to anyone who passes by. Locking your screen is one of the easiest steps to keep someone off your computer. When you step away from your desk press the “alt + ctrl + delete keys” and choose lock computer. You will need your Windows login password or an administrator account to unlock the computer for use. A way to automate this step is to set your screen saver to require a password when you return. If you working in an area with other people let

them know you are leaving and to keep an eye on your area. If they see someone they do not know approach your computer, have them stop that person and see what they need. Immediately report any suspicious activities to your supervisor or the ResNet staff.

Sensitive data:

In some cases the information you work with should not be disclosed to anyone else. In these cases you should take special care with the above instructions. Also you should be very careful with "Web Surfing" and make sure that sites you are going to are sites you can trust. These sites are ones you receive in documentation from a company, that are recommended by your department or the university, or by using another computer connected to the Internet to research the site.

Always use your resources:

The information provided here is just a small sample of computer security. If there is anything that you are unsure about or would like more information please contact ResNet. You may contact the ResNet Helpdesk at 994-1929 or you may send your question in an E-mail to resnet@montana.edu.