Information Management Resource Kit

Module on Building Electronic Communities and Networks

UNIT 4. DESIGNING AN ONLINE COMMUNITY

LESSON 4. ONLINE SECURITY AND PRIVACY

NOTE

Please note that this PDF version does not have the interactive features offered through the IMARK courseware such as exercises with feedback, pop-ups, animations etc.

We recommend that you take the lesson using the interactive courseware environment, and use the PDF version for printing the lesson and to use as a reference after you have completed the course.

Objectives

At the end of this lesson, you will be able to:

- identify virus and related security risks your computer could be exposed to;
- understand risks connected to catastrophic or limited loss of information;
- select back-up techniques for a specific situation; and
- understand the principles of access controls for an online community.

Introduction

Computers and the Internet offer individuals, groups and organizations a highly effective way of working together and sharing information.

The more dependent you become on these tools, however, the more important it becomes for you to learn about **possible risks and how to deal with them**.

Learning more about how to reduce these risks by looking after and protecting your computer is the first step on the way to reducing the risks for your organization or online community.

In this lesson, you will learn some basic methods for ensuring system security for your own computer and those of the community members.

The risks

Apart from physical damage, computer operating systems – the collection of programs and files that make the computer work – can easily be damaged by:

- the **user** of the computer system, or
- computer **viruses or other programs** that exploit security weaknesses in the computer system or Internet connection; these programs are collectively known as **malware** (“MALicious softWARE”).

Malware can damage your software, hardware and information. It can also damage the reputation of you and your organization. It takes time and money to repair this damage – costs community organizations can ill afford. It is much better to try to prevent it from happening in the first place.

How malware works

Malware works in the same way as a “normal” computer program - by making the computer's processor carry out a sequence of commands. Unlike a normal program, however, malware is maliciously designed to **change the configuration** of the system or **cause other damage,** sometimes extensive.

User activated viruses

These viruses have to be activated by the user. In other words, the user has to run the program or open the file which contains the virus code. Most early viruses and some current ones were of this type.

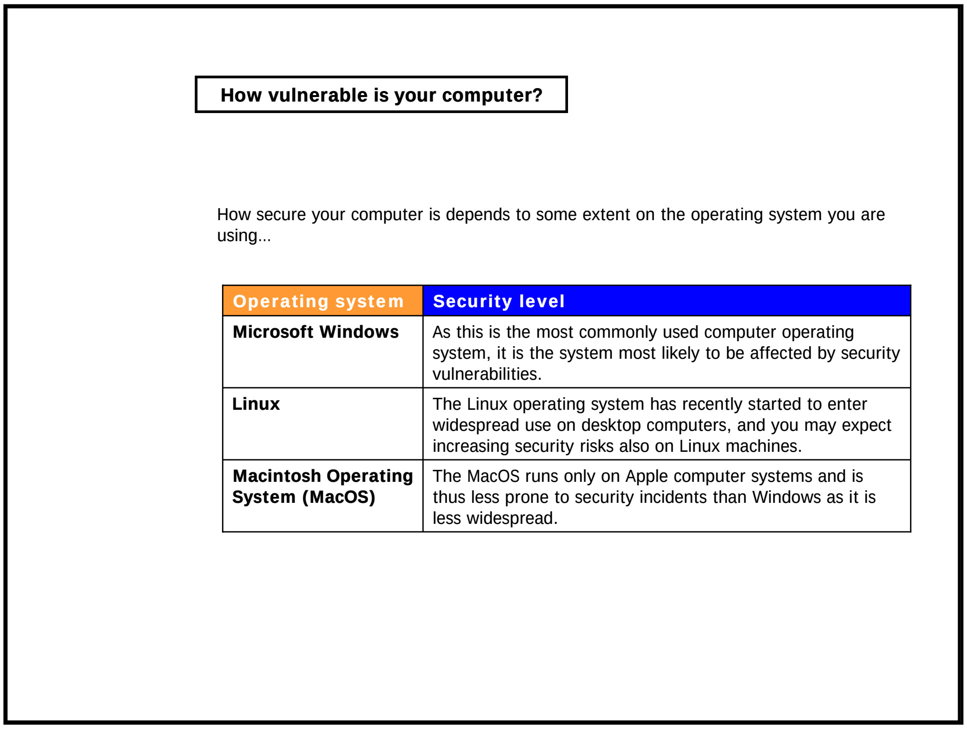
Automated virus activation

As computer operating systems have developed, more things are being done automatically by the operating system. This means that the malware program can be run accidentally by the user, or that the operating system may be tricked into running the program because it appears to be a legitimate program.

As malware has evolved, **different types of program** have been developed: Viruses, Worms, Trojans, Spyware, etc.

Would you like to know more about malware?

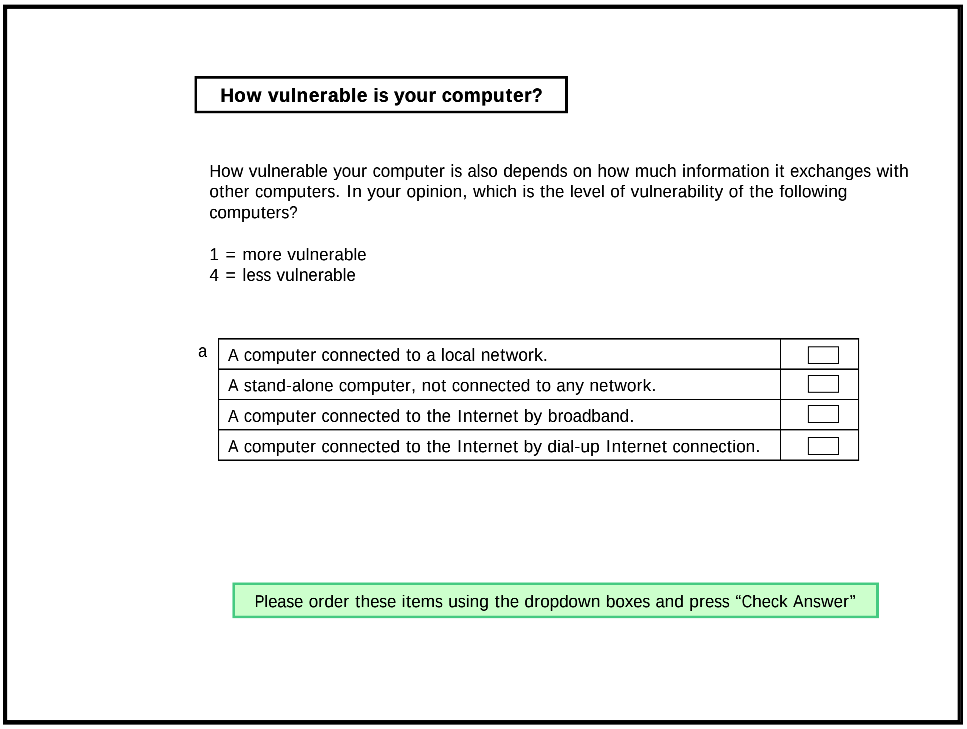
See Annex 4.4.1 for a mini-lesson on Viruses, Worms, Trojans, Spyware and how you get infected by them.



How vulnerable is your computer?

How secure your computer is depends to some extent on the operating system you are using...

Operating system	Security level
Microsoft Windows	As this is the most commonly used computer operating system, it is the system most likely to be affected by security vulnerabilities.
Linux	The Linux operating system has recently started to enter widespread use on desktop computers, and you may expect increasing security risks also on Linux machines.
Macintosh Operating System (MacOS)	The MacOS runs only on Apple computer systems and is thus less prone to security incidents than Windows as it is less widespread.



How vulnerable is your computer?

How vulnerable your computer is also depends on how much information it exchanges with other computers. In your opinion, which is the level of vulnerability of the following computers?

1 = more vulnerable
4 = less vulnerable

a

A computer connected to a local network.	□
A stand-alone computer, not connected to any network.	□
A computer connected to the Internet by broadband.	□
A computer connected to the Internet by dial-up Internet connection.	□

Please order these items using the dropdown boxes and press “Check Answer”

How can you reduce your vulnerability?

Reducing your vulnerability means taking a combined approach, as no one tool or technique on its own offers sufficient protection.

See next slides for more information on each technique

Run anti-virus software and keep it up to date
Anti-virus programs monitor files on your computer and information that enters via the network to see if they contain malware code…

Configure your software to reduce security risks
As the major hazard from malware today comes from use of the Internet, it is important to access it in a way that reduces the chances of malware being activated by your system…

Get system updates/ "patches"
Malware writers exploit security flaws or "holes" in software programs. As new flaws are discovered, program writers develop patches to fix them…

Be cautious about opening e-mail attachments
The greatest risk is from e-mail attachments that contain programs…

How can you reduce your vulnerability?

Run anti-virus software and keep it up to date

Anti-virus programs monitor files on your computer and information that enters via the network to see if they contain malware code. If the anti-virus program finds malware code it will "quarantine" the file or e-mail to prevent the code it contains being executed. Most of the anti-virus programs in common use are for Windows as it has the greatest problems with malware.

Malware changes or "mutates" over time as virus writers adapt and improve the code to counter new developments in anti-virus software. As a consequence, it is necessary to regularly update the anti-virus program. How often usually depends upon which program you buy, and how much you spend. Usually the more expensive anti-virus programs give more updates, and updating might take place automatically whilst your computer is connected to the Internet.

Free anti-virus tools and resources
The most widely-used anti-virus tools are commercial packages such as Norton and McAfee and are relatively inexpensive. There are, however, a few free tools available, and some commercial anti-virus vendors also offer free online scanning tools. Free tools can be as effective as commercial ones, but may require more effort on the part of the user – for example, they may not provide automatic updates, or may not scan e-mail messages.
Two free tools worth considering are **AntiVir® Personal Edition Classic** and **Trend HouseCall online scan** (see Online Resources at the end of this lesson).

How can you reduce your vulnerability?

Configure your software to reduce security risks

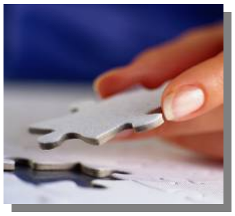
As the major hazard from malware today comes **from use of the Internet**, it is important to access it in a way that reduces the chances of malware being activated by your system. This method will also reduce the risks from new viruses that might not be picked up by anti-virus software.

You should try and do the following to minimise the risk from malware...

- Both e-mail and web browsing programs contain **“preferences” menus** where the user can enable or disable certain features. Here you can disable the use of scripting languages completely, or allow them only from certain trusted sites. This reduces the risk of uploading programs whilst online.
- Word processor or spreadsheet programs allow the use of “macros”, user-defined programs that perform simple functions, but which can be abused by virus writers. For this reason any program that uses macros should have the **macro facility turned off** to prevent the spread of macro-viruses through e-mail attachments. Usually if a file does have a macro you will be warned and given the option of opening it with (if you trust the files source) or without the macro enabled.

How can you reduce your vulnerability?

Get system updates/ “patches”



Malware writers exploit security flaws or “holes” in software programs. As new flaws are discovered, program writers develop **patches** to fix them.

A patch is a small program that re-writes the code that makes up the operating system and other programs to prevent the malware code from gaining access or being executed.

Sometimes patches are issued when a security concern arises, but often a patch only becomes available following a serious virus outbreak. This is because most security flaws are unknown, and only become apparent when malware writers discover them and use a particular flaw to develop a new type of virus.

System patching is not fool-proof, but it is the most effective way of preventing malware from affecting computer systems. For this reason it is important to regularly check if new security concerns have arisen, and whether new patches or updates have become available for your operating system.

How can you reduce your vulnerability?

Be cautious about opening e-mail attachments

The greatest risk is from e-mail attachments that contain programs. Sometimes these have a double file name extension to confuse the user (e.g. ".doc.vbs"). Make sure that your e-mail settings do not allow attachments to be opened automatically.

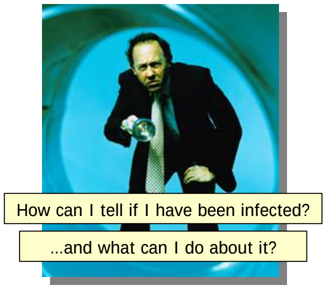
You also can decide to only receive attachments **by prior arrangement**, so you can delete any e-mail with an attachment unless that person has previously informed you. To make this clear you should put a note in your e-mail signature that attachments are only received by arrangement.

Most viruses circulate with e-mail "spoof" headers: the virus takes e-mail addresses from the infected computers and puts them as senders into the messages carrying the infected attachments. This means that even if the message appears to come from someone you know, you still need to be cautious about opening the attachment.

Date sent:	Fri, 25 Jun 2004 10:41:10 -0300
From:	**Thembi Radebe <thembi@immunization.org>**
To:	celeste@ngo.org
Subject:	read this

As precautions you can:
- use an anti-virus program that scans e-mail attachments as well as the files on your hard drive;
- avoid vague subject headings, and provide meaningful descriptions of attachments. For example, "Attached are the minutes of the staff meeting, 25 June 2004" is better than "read this".

How to deal with virus infections?



How can I tell if I have been infected?

...and what can I do about it?

Of course, even if you pay attention to security aspects, your computer could be infected.

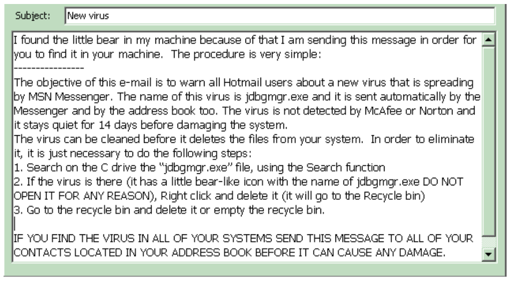
Symptoms of infection vary, and many symptoms can also be the result of software or hardware problems which are not malware-related. Your computer might slow down or stop responding, or keep restarting every few minutes.

If you suspect you have been infected by a virus...

- Perform a **scan using an anti-virus software**, and follow any instructions. If you do not have up to date anti-virus software on your pc, consider running an online scan.
- If you are in a situation where knowledgeable computer advice and support is available (e.g. in your office), **turn the computer off and seek advice**. Virus infection could require action over and above using an anti-virus program.
- Do **not exchange files** with other computers: you could infect them too!

Virus hoaxes

Imagine you receive this e-mail message:



Subject: New virus

I found the little bear in my machine because of that I am sending this message in order for you to find it in your machine. The procedure is very simple:

The objective of this e-mail is to warn all Hotmail users about a new virus that is spreading by MSN Messenger. The name of this virus is jdbgmgr.exe and it is sent automatically by the Messenger and by the address book too. The virus is not detected by McAfee or Norton and it stays quiet for 14 days before damaging the system.

The virus can be cleaned before it deletes the files from your system. In order to eliminate it, it is just necessary to do the following steps:

1. Search on the C drive the "jdbgmgr.exe" file, using the Search function
2. If the virus is there (it has a little bear-like icon with the name of jdbgmgr.exe DO NOT OPEN IT FOR ANY REASON), Right click and delete it (it will go to the Recycle bin)
3. Go to the recycle bin and delete it or empty the recycle bin.

IF YOU FIND THE VIRUS IN ALL OF YOUR SYSTEMS SEND THIS MESSAGE TO ALL OF YOUR CONTACTS LOCATED IN YOUR ADDRESS BOOK BEFORE IT CAN CAUSE ANY DAMAGE.

What do you do?

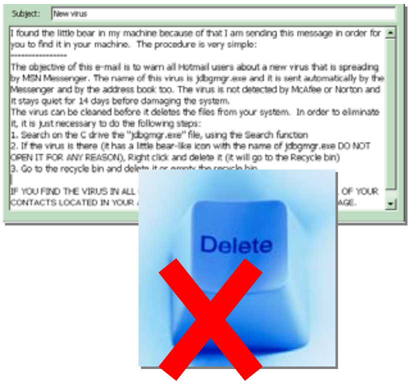
□ Search for the file and delete it if you find it.
□ Call your computer support division or Internet service provider.
□ Forward the message to everyone in your address book so that they don't get the virus too.
□ Visit an anti-virus Web site to look for information.
□ Turn off your computer immediately.

Please select the answers of your choice (2 or more) and press Check Answer

Virus hoaxes

What we have seen is an example of **virus hoaxes**.

To most users the programs and files that make-up the operating system of a computer are a mystery. This creates the potential for **fake warnings about viruses or other malware** to be sent out via e-mail. Then, through endless forwarding of the original e-mail by friends and colleagues, the hoax spreads just like an ordinary virus.


Subject: New virus

I found the little bear in my machine because of that I am sending this message in order for you to find it in your machine. The procedure is very simple:

The objective of this e-mail is to warn all Hotmail users about a new virus that is spreading by MSN Messenger. The name of this virus is jdbgmgr.exe and it is sent automatically by the Messenger and by the address book too. The virus is not detected by McAfee or Norton and it stays quiet for 14 days before damaging the system.

The virus can be cleaned before it deletes the files from your system. In order to eliminate it, it is just necessary to do the following steps:

1. Search on the C drive the "jdbgmgr.exe" file, using the Search function
2. If the virus is there (it has a little bear-like icon with the name of jdbgmgr.exe DO NOT OPEN IT FOR ANY REASON), Right click and delete it (it will go to the Recycle bin)
3. Go to the recycle bin and dele

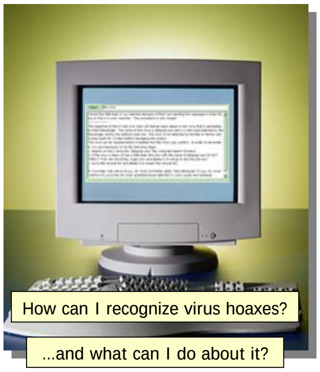
IF YOU FIND THE VIRUS IN ALL OF YOUR
CONTACTS LOCATED IN YOUR AGE.

Many virus hoaxes take the form of a message that states that if a certain file is present on your computer then you have contracted a virus.

The "solution" proposed is to delete the file from the system. However, the file you are asked to delete by the hoax message is a legitimate file.

Deleting it can mean that at some time in the future the operating system will fail to function properly because of the missing file.

Virus hoaxes



How can I recognize virus hoaxes?

...and what can I do about it?

Hoax virus messages tend to share a number of characteristics, the most common one being that they ask you to forward the message to “everyone in your address book”.

Do not forward the message! If you receive a virus warning, do one or all of the following:

- Check out the warning on an anti-virus Web site. Producers of anti-virus software often post information about both viruses and virus hoaxes on their sites.
- Ask your computer support division or your Internet service provider for confirmation.
- Check one of several sites that catalogue virus hoaxes (http://www.vmyths.com/)

Viruses and your online community

E-mail based communities such as listservers are vulnerable to the spread of both real viruses, and virus hoaxes.

As manager or facilitator of an online community, you can…

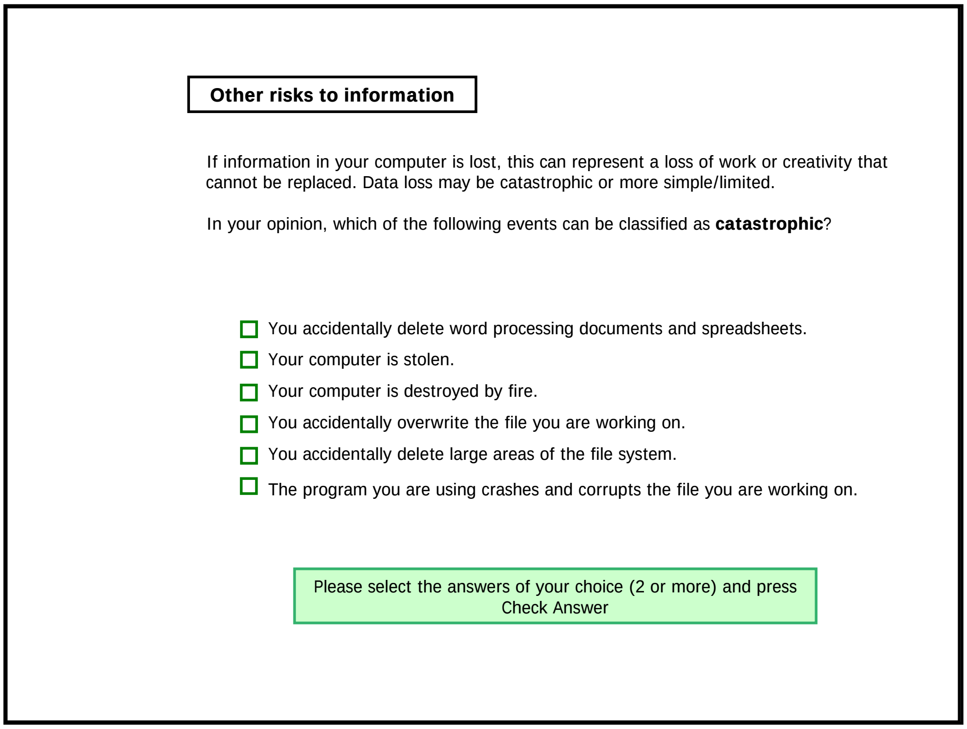
- Check that your listserver host (free, commercial or in-house) has **anti-virus** protection measures in place.
- Set a **list policy** on forwarding virus-related information.
- Place restrictions on posting **attachments** to your community’s e-mail spaces.
- Help **community members** understand virus- and malware related threats and how to deal with them.

Example of list policy

FAQ:
Frequently Asked Questions
about the DIGITALDIVIDE discussion list

The following subjects are considered inappropriate and may be rejected for publication:
- Private posts to individual list members (unless they're a clear benefit to the list as a whole).
- For-profit advertisements of any type whatsoever.
- Administrative questions (post these directly to the moderator).
- Computer virus warnings without adequate verification (see below).

Most of the above examples are straightforward, but I'd like to explain the virus warning ban. Every now and then you may receive an e-mail from someone warning you about some new computer virus, encouraging you to spread the word. In 99.9% of all cases, these messages are hoaxes. The virus itself doesn't exist; rather, the hundreds of thousands of e-mail generated by people spreading the word about it is the actual virus, taking up precious Internet bandwidth. If you are determined to post a warning, though, please check the Virus Warning Web site at http://www.vmyths.com to confirm or debunk the virus' existence.



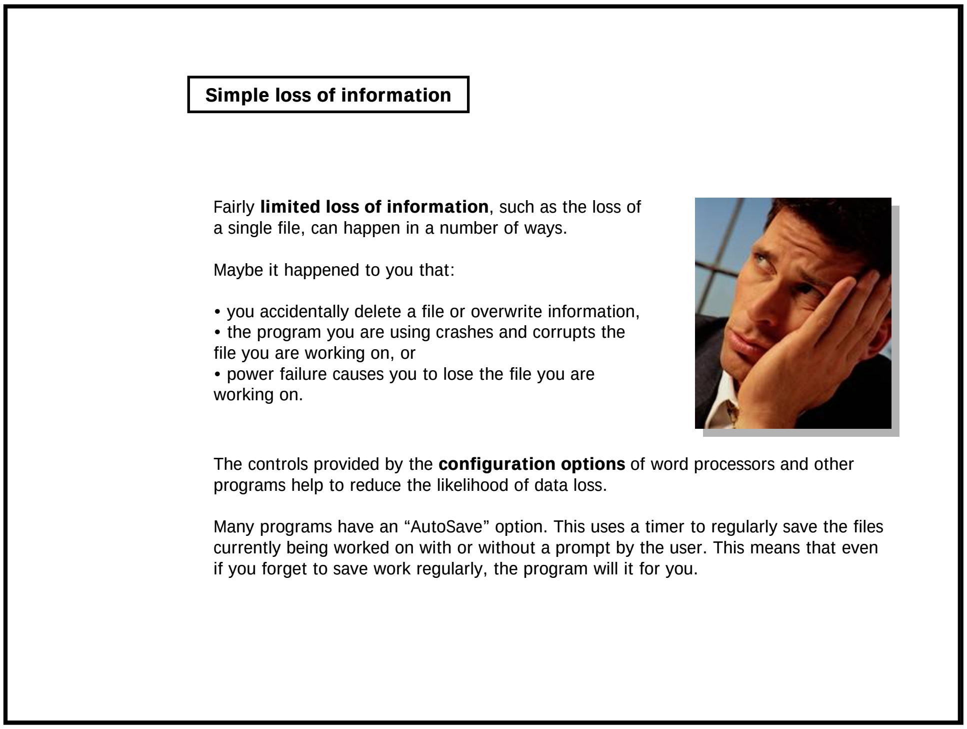
Other risks to information

If information in your computer is lost, this can represent a loss of work or creativity that cannot be replaced. Data loss may be catastrophic or more simple/limited.

In your opinion, which of the following events can be classified as **catastrophic**?

□ You accidentally delete word processing documents and spreadsheets.
□ Your computer is stolen.
□ Your computer is destroyed by fire.
□ You accidentally overwrite the file you are working on.
□ You accidentally delete large areas of the file system.
□ The program you are using crashes and corrupts the file you are working on.

Please select the answers of your choice (2 or more) and press Check Answer



Simple loss of information

Fairly **limited loss of information**, such as the loss of a single file, can happen in a number of ways.

Maybe it happened to you that:

- you accidentally delete a file or overwrite information,
- the program you are using crashes and corrupts the file you are working on, or
- power failure causes you to lose the file you are working on.

The controls provided by the **configuration options** of word processors and other programs help to reduce the likelihood of data loss.

Many programs have an “AutoSave” option. This uses a timer to regularly save the files currently being worked on with or without a prompt by the user. This means that even if you forget to save work regularly, the program will it for you.

Simple loss of information

How to enable “AutoSave” option

How you enable these features varies from program to program. You can usually find these settings in an “options” or “configuration” menu, and are variously called “security” or “saving”. In general they all work the same way, with the exception that some programs set up a folder specifically to hold the backup copies of files.

For example, in order to set AutoSave in MS Word (Office XP), you have to click on the **Save** tab in the **Tools > Options** dialogue.

Set the auto-save feature to work every ten to fifteen minutes. With the auto-save feature enabled, if there is a problem with the computer or the program you can restart and load the last saved version of the file.
As well as saving, you have the option of creating “backup copies”. If you use this option, the last saved version of the file is renamed to be the backup file. The most recent version working file is saved as a new file with the same name.
This means that if you realise that you have accidentally over-written a file, or saved an incomplete or corrupted version, you can re-load the backup version of that file and recover a large part of the content.

Catastrophic loss of information

In security terms, a **catastrophic failure** is an event that leads to the large scale loss of or damage to information and equipment.

One way is that the user accidentally deletes **large areas of the file system**.

It is quite easy to reduce this kind of risk: if users are allocated a specific “workspace” for their data files, that is an area in the storage system that they use exclusively for their work, then they should have no need to manipulate any other files on the system.

Most operating systems use the idea of a workspace, for example the “My Documents” folder in Windows. Ensure that you use this space and this space alone for your files.

Catastrophic loss of information

OTHER REASONS FOR CATASTROPHIC INFORMATION LOSS

Catastrophic loss of information can also happen when:

- a fault with the operating system, such as deleting an important system file or because of a virus infection, corrupts data or renders the computer system unusable;
- a computer develops a hardware fault, such as a hard disk failure, that will lose all the information held on the system;
- the computer is stolen;
- the computer is damaged by a power surge or is destroyed in a fire or some other catastrophic event.

Problems such as viruses, hardware faults and theft can be dealt with by **regularly backing-up** of the information held on the computer.

Backing up systems

Backing up your system means **making copies of the data** stored on it. That way, if files on your computer are damaged, they can be restored from the copies: the data loss will be confined to the period between the date of the fault and the last backup. If your computer is destroyed or stolen the files can be uploaded to your replacement computer.

It is advisable to keep backup copies **in a different location**, so that data are protected even if there is a catastrophe such as a fire.

There are many ways to backup information; one of the most important considerations is to choose a storage medium with **sufficient capacity** to store all the data you need to back up.

More information about back-up tools and techniques (PDF FILE)

Backing up systems

As a computer user, you should backup **all your own data files** (e.g. word processing documents, spreadsheets and pictures). Selecting files to be backed up is much easier if you store your data files in your workspace.

In order to save time, you don't need to backup redundant information such as:

- saved web pages that can be downloaded from the Web,
- information of which there are CD copies, and
- files such as programs (but you should ensure that the original disks are kept in a safe place along with any relevant licenses).

Network administrators are responsible for ensuring that **all** data on the network is backed up regularly.

Regular backup

In the situation where you have good backup software (e.g. Norton Ghost) and plenty of storage, it is worth backing up your entire system. In fact, reinstalling all the software and re-configuring it takes a long time, and can be brought back from a backup much more quickly.

Moreover, some software applications now require you to activate them over the Internet before you can use them, as an antipiracy measure. Re-activating them after a system crash can cause some problems (e.g. you could need to call the vendor before using the software again).

Backing up systems

Segregating information according to its **sensitivity** is good practice for individual computer users, and essential for organizational systems. Disclosing highly sensitive information (such as personal information or financial data) publicly, can damage your organization. This information should be **segregated and backed-up separately**.

It isn't just that the backup copies need to be stored in a more secure manner. When the backup copy is replaced with a new backup, the old backup media must be securely erased or, in the case of write-once media like CD-ROMs, destroyed. Never re-use media which has been used for backing up highly sensitive data for other purposes.

Another reason to segregate data is to comply with **legal requirements**. For example, within the European Union, the Data Protection Directive creates minimum standards for the storage and disclosure of information on computer systems.

Backing up systems

Imagine you are backing-up data on your computer. How do you treat following data?

a Programs of which you have original disks and licenses.

Files containing personal information on your consultants.

Your own Word documents and spreadsheets.

Web pages you have downloaded from the Internet.

Back-up in a more secure manner and securely erase old copies. 1

Don't back-up.

Don't back-up.

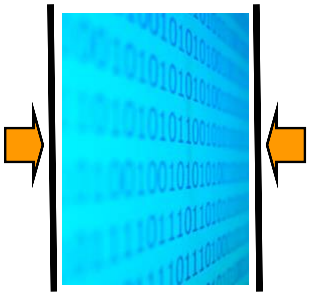
Back-up in a straightforward fashion.

Click on each option, drag it and drop it in the corresponding box.

When you have finished, click on the Check Answer button.

Compression and archiving

Compression and archiving are useful techniques used to store and/or transmit data. Compression removes repeated sequences of data in order to reduce the size of files. Archiving tools combine a collection of files into a single file, and generally compress the file at the same time.



Compression tools add an extra level of risk to the backup process. For example, you might compress one hundred files into a single archive in order to fit those files on a single disk. If the information in the backup copy is corrupted you may lose all one hundred files in the archive, not just the one or two that might have resulted from those same files being stored on the backup disks as individual files.

How or when you use these programs is thus a matter of balancing your storage space constraints with your need for reliable backups.

Would you like to know more about compression and archiving?

See Annex 4.4.2 for a mini-lesson on compressing and archiving files with WinZip

Compression and archiving

How compression works

Most computer files contain information which is repeated many times. For example, in your organization's annual report, the name of your organization might appear 50 times. Common words such as "the" and "and" will be repeated many times over.

Every letter or other character used in a document takes up space. A compression program allocates a number to each repeated word. For example:

And	1
Organization	2
But	3

To compress the file, the program replaces the repeated words with the shorter codes, thus making the file significantly smaller.

To decompress the file, the program restores the complete versions of the words.

Backing up while on the move

More and more information devices are becoming portable - this increases the risk that the information they contain will be lost. Most significantly, a mobile device (such as a notebook) may be damaged or stolen. You can reduce the risk by…

Conducting a **conventional backup**. The problem here is that you have to carry backup disks, and these may also be lost. However, if your device has the capability to create CDs, or if you use a removable external storage device, creating backups is very simple.

Backing-up **over the Internet**. There are various options to backup over the Internet: you can create an archive and then e-mail it, or use a file transfer protocol (FTP) service to move the data to a secure server. The main disadvantage of this method is that for large amounts of data you will need a broadband connection. Also, data you send across the Internet is not secure, and if you are transferring sensitive information you will need to take measures such as encryption.

Developing a backing up policy

To be effective, backing up must be done **regularly**.
That doesn't just mean backing up at fixed time intervals - it also means backing up at particularly significant points in your workflow.

For example:

• it's a good idea to back up the file related to a particular work activity when that activity is complete, or when important milestones have been reached; and

• when carrying out regular tasks, such as accounting or stock taking, it's a good idea to carry out a backup after this is complete to ensure those records are preserved.

Both individuals and organizations should have backing up policies.

Organizational backing up policies

It is important that organizations adopt a clear policy on the responsibilities for backing up the information held on computer systems and when this should take place – and that any necessary training is provided for staff. There is no one correct model for a technical security policy. What matters is that the way the information backup is produced is regular, reliable, and achievable given the equipment that is available.
What is important is that:
• the backup copies are securely stored to prevent their loss, or tampering with their content;
• copies of the backup are kept at another secure location; this need not be done each time a backup takes place, but it should work around a cycle that ensures that a catastrophic loss of data will not be so serious that it prejudices the work of the organization;
• data should be segregated according to its sensitivity, in order to reduce the scale of the backing up operation and to demonstrate compliance with any relevant legal requirements on the protection of computerized information.

Backing up systems

Your friend Sanjay is worried about the security of the data on his Windows computer at home. Which of the following would you suggest to him?

□ He should regularly backup all the data and operating system files on his computer.

□ He should regularly backup his data files such as word processing documents and spreadsheets.

□ He should store his documents in the “My Documents” folder.

□ He should store copies of his program files and licenses in a safe place.

□ He should never use zip archives to store files for backup purposes.

Please select the answers of your choice (2 or more) and press Check Answer

Action for your online community

The risks outlined above can affect your online community or network in a number of ways.

Your online spaces may store a wealth of information: e.g., contact information about participants, or the resources available through your Web site. Losing this information would certainly have a negative effect on your community!

Moreover, if community members are unable to deal with technical security problems on their own computers, they may be unable to participate actively in the community.

Once you are familiar with the basics of technical security, apply this knowledge to your online community.

- Ensure that the systems which store your online community's information are regularly backed up.

- Build capacity among community members by raising awareness of the risks and the ways of minimizing them.

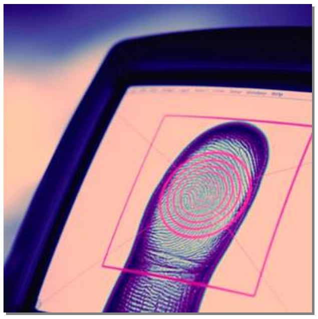
Access control

Access control is all about ensuring that information is **accessible to those who are authorized** to see it, but not to those who are not. Access controls help you maintain **computer and online privacy**.

On the next screens we will look at the main type of access controls you should consider: **passwords** and **firewalls**.

In general, do not prevent access to information or resources unless there is a good reason to: creating unnecessary barriers will just make additional work and wasted effort.

Access control



Passwords are a way of checking that the person trying to use a computer (or access an online database, or change the setting of an e-mail list) is the person they say they are, and that they have a right to access the information concerned or perform a particular task.

Although passwords are not infallible, they are an important basic step towards protecting computers, files, networks, and online spaces such as Web sites and discussion boards.

Would you like to know more about passwords?

See Annex 4.4.3 for a mini-lesson on using passwords for computers, files, online spaces and networks

Access control

A computer which is connected to the Internet is open to unauthorized access via this connection. Using a **firewall** helps prevent unauthorized access and of restricting it to particular services or programs.

Obviously you don’t want to block all network traffic to and from your computer. Rather, you need to ensure that “good” traffic (such as your e-mail, and the web pages you want to view) can move freely, while “bad” (i.e. unauthorized) traffic is kept out.

Firewalls are an essential tool in securing every computer connected to the Internet.

Access control

Who might be trying to access my computer through its Internet connection? And why?

Sometimes computer systems are the direct target of would-be unauthorized users – for example, the computers of banks or government departments might be targeted in order to steal personal information.
The average computer user or organization is unlikely to be targeted directly.
More common is that unscrupulous people use tools which scan the internet for unprotected computers, and then exploit these insecurities for a number of purposes, such as:
accessing data such as passwords;
• transmitting worms and other malware; and
• using your connection for mass mailings of junk e-mail ("spam").

Firewalls

Organizations which are running local area networks need to ensure that online security plans include implementation of firewalls.
Individuals or organizations with Internet access on standalone (i.e., non-networked) computers should install **personal firewall software** to identify and block unauthorized access.
Please remember that, as firewalls are often implemented in software, they are subject to bugs and vulnerabilities just like any other piece of software. As consequence, they should be used in addition to and not substituting other good security practices.
Although Windows XP includes a firewall tool, dedicated tools such as ZoneAlarm provide a higher level of security and more flexibility.
ZoneAlarm is highly-recommended personal firewall software, and is free for individual and not-for-profit use:
http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp

Access control

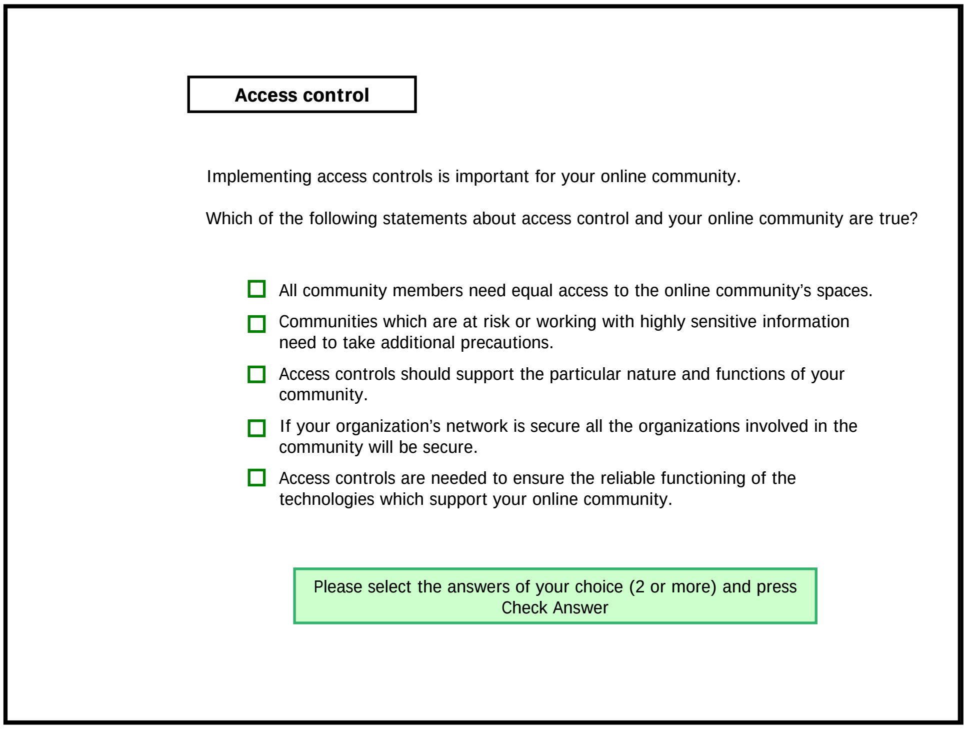
What are the implications of access controls for your **online community**?

Access controls are needed to ensure the reliable functioning of the **technologies** which support your online community: unauthorized access can result in damage to your systems, and could mean that your online spaces stop working.

Access controls should be configured to support your **particular** community. Communities may be very public, very private or contain both private and public online spaces. More sophisticated access controls are needed by communities that are particularly at risk or that work with sensitive information (human rights, health records, etc.).

Ensure that **sensitive** information relating to your online community is secure: implement appropriate access controls on your own computer, and ensure that those responsible for other computers housing this information (e.g. your Internet service provider) do the same.

Finally, try and help raise **awareness of the need for access controls** among community members.



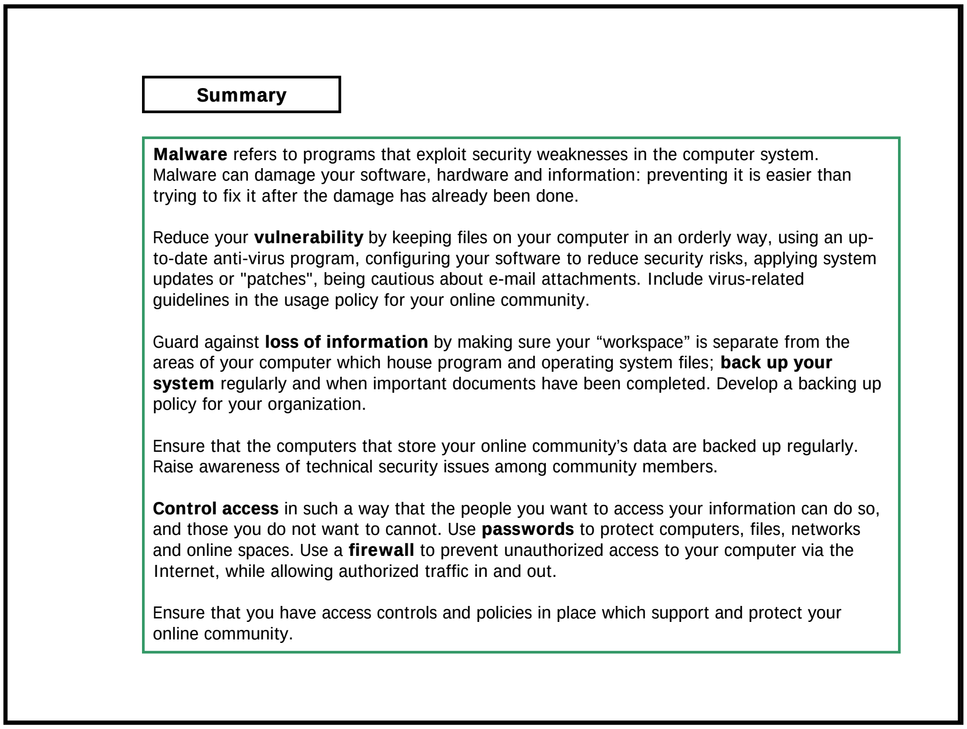
Access control

Implementing access controls is important for your online community.

Which of the following statements about access control and your online community are true?

- □ All community members need equal access to the online community's spaces.
- □ Communities which are at risk or working with highly sensitive information need to take additional precautions.
- □ Access controls should support the particular nature and functions of your community.
- □ If your organization's network is secure all the organizations involved in the community will be secure.
- □ Access controls are needed to ensure the reliable functioning of the technologies which support your online community.

Please select the answers of your choice (2 or more) and press Check Answer



Summary

Malware refers to programs that exploit security weaknesses in the computer system. Malware can damage your software, hardware and information: preventing it is easier than trying to fix it after the damage has already been done.

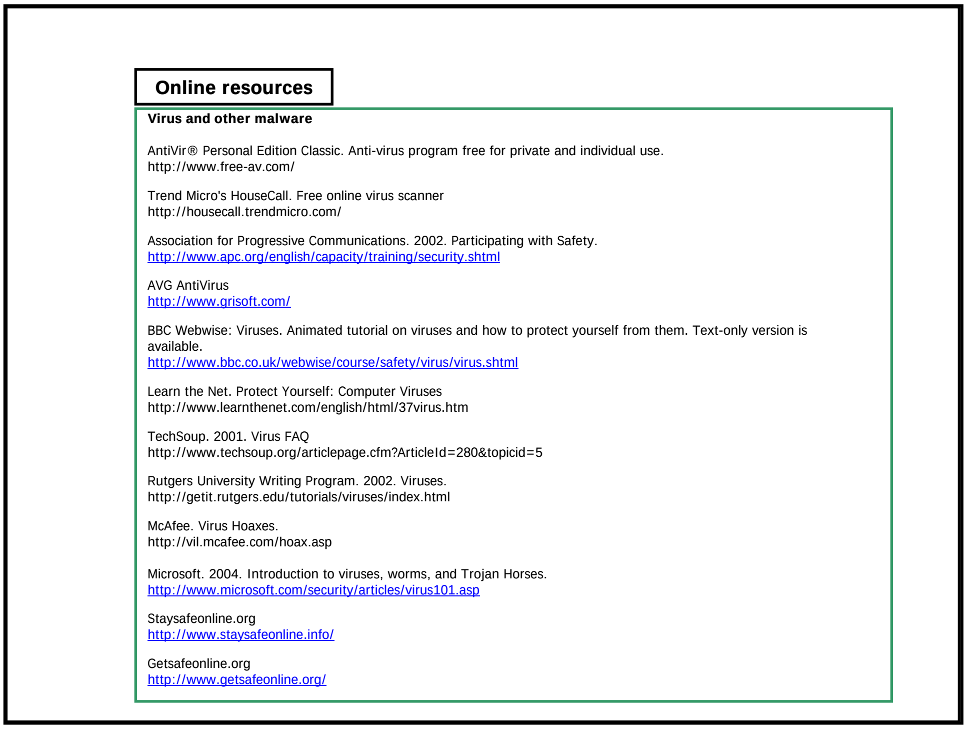
Reduce your **vulnerability** by keeping files on your computer in an orderly way, using an up-to-date anti-virus program, configuring your software to reduce security risks, applying system updates or "patches", being cautious about e-mail attachments. Include virus-related guidelines in the usage policy for your online community.

Guard against **loss of information** by making sure your “workspace” is separate from the areas of your computer which house program and operating system files; **back up your system** regularly and when important documents have been completed. Develop a backing up policy for your organization.

Ensure that the computers that store your online community's data are backed up regularly. Raise awareness of technical security issues among community members.

Control access in such a way that the people you want to access your information can do so, and those you do not want to cannot. Use **passwords** to protect computers, files, networks and online spaces. Use a **firewall** to prevent unauthorized access to your computer via the Internet, while allowing authorized traffic in and out.

Ensure that you have access controls and policies in place which support and protect your online community.



Online resources

Virus and other malware

AntiVir® Personal Edition Classic. Anti-virus program free for private and individual use.
http://www.free-av.com/

Trend Micro's HouseCall. Free online virus scanner
http://housecall.trendmicro.com/

Association for Progressive Communications. 2002. Participating with Safety.
http://www.apc.org/english/capacity/training/security.shtml

AVG AntiVirus
http://www.grisoft.com/

BBC Webwise: Viruses. Animated tutorial on viruses and how to protect yourself from them. Text-only version is available.
http://www.bbc.co.uk/webwise/course/safety/virus/virus.shtml

Learn the Net. Protect Yourself: Computer Viruses
http://www.learnthenet.com/english/html/37virus.htm

TechSoup. 2001. Virus FAQ
http://www.techsoup.org/articlepage.cfm?ArticleId=280&topicid=5

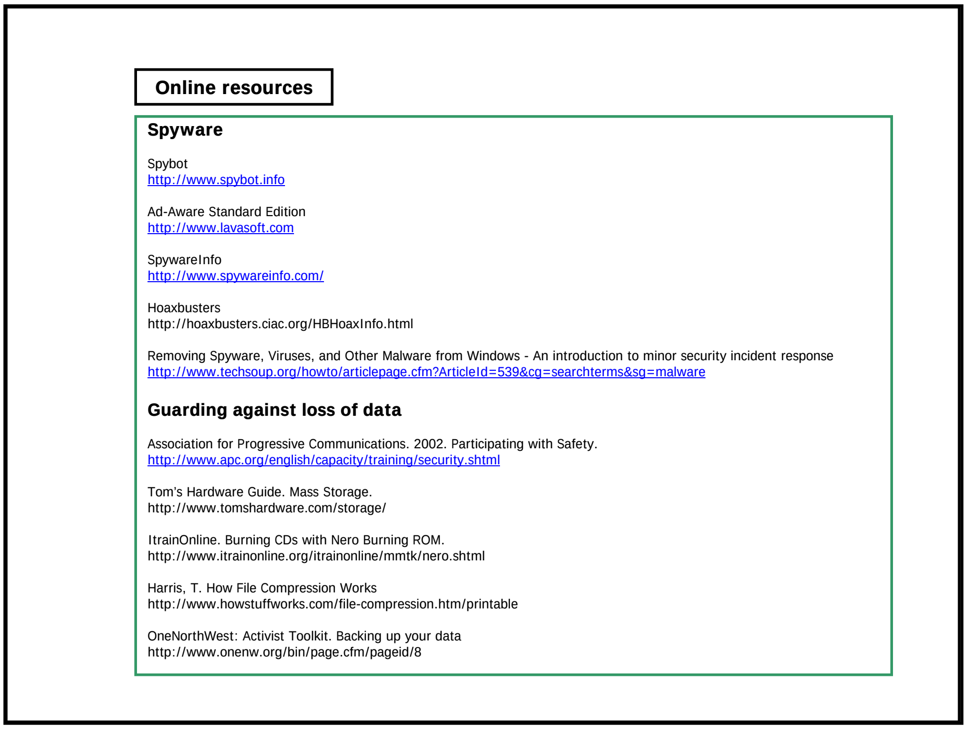
Rutgers University Writing Program. 2002. Viruses.
http://getit.rutgers.edu/tutorials/viruses/index.html

McAfee. Virus Hoaxes.
http://vil.mcafee.com/hoax.asp

Microsoft. 2004. Introduction to viruses, worms, and Trojan Horses.
http://www.microsoft.com/security/articles/virus101.asp

Staysafeonline.org
http://www.staysafeonline.info/

Getsafeonline.org
http://www.getsafeonline.org/



Online resources

Spyware

Spybot
http://www.spybot.info

Ad-Aware Standard Edition
http://www.lavasoft.com

SpywareInfo
http://www.spywareinfo.com/

Hoaxbusters
http://hoaxbusters.ciac.org/HBHoaxInfo.html

Removing Spyware, Viruses, and Other Malware from Windows - An introduction to minor security incident response
http://www.techsoup.org/howto/articlepage.cfm?ArticleId=539&cg=searchterms&sg=malware

Guarding against loss of data

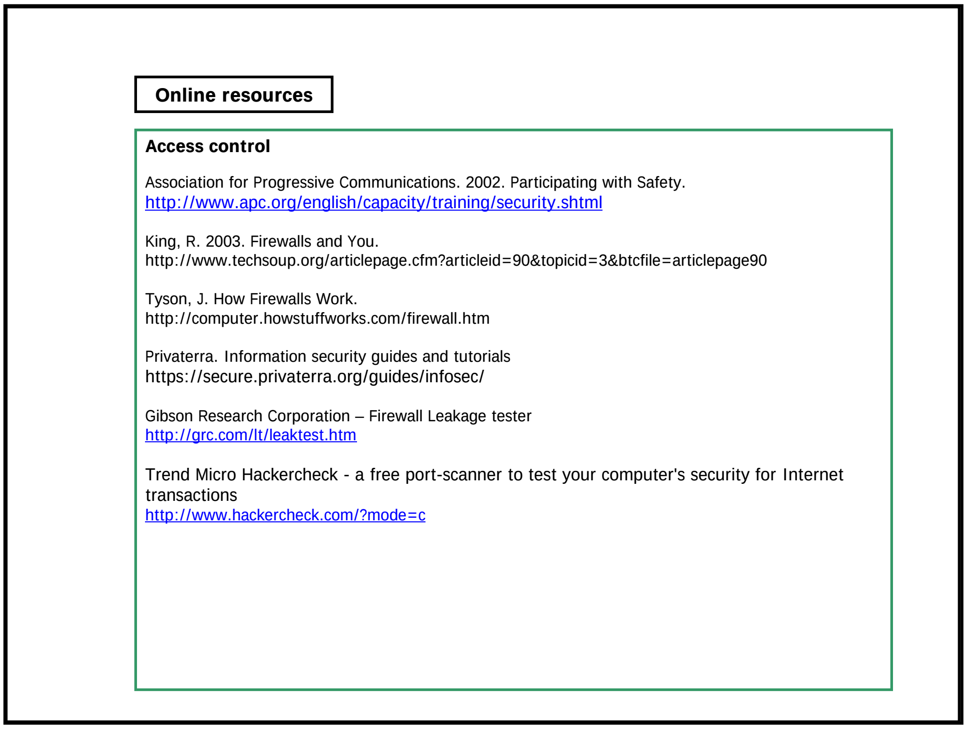
Association for Progressive Communications. 2002. Participating with Safety.
http://www.apc.org/english/capacity/training/security.shtml

Tom's Hardware Guide. Mass Storage.
http://www.tomshardware.com/storage/

ItrainOnline. Burning CDs with Nero Burning ROM.
http://www.itrainonline.org/itrainonline/mmtk/nero.shtml

Harris, T. How File Compression Works
http://www.howstuffworks.com/file-compression.htm/printable

OneNorthWest: Activist Toolkit. Backing up your data
http://www.onenw.org/bin/page.cfm/pageid/8



Online resources

Access control

Association for Progressive Communications. 2002. Participating with Safety.
http://www.apc.org/english/capacity/training/security.shtml

King, R. 2003. Firewalls and You.
http://www.techsoup.org/articlepage.cfm?articleid=90&topicid=3&btcfile=articlepage90

Tyson, J. How Firewalls Work.
http://computer.howstuffworks.com/firewall.htm

Privaterra. Information security guides and tutorials
https://secure.privaterra.org/guides/infosec/

Gibson Research Corporation – Firewall Leakage tester
http://grc.com/lt/leaktest.htm

Trend Micro Hackercheck - a free port-scanner to test your computer's security for Internet transactions
http://www.hackercheck.com/?mode=c

Annex 4.4.1
Mini-lesson: Types of Malware

As malware has evolved, different types of program have been developed:

Name	Description	How do you get infected?
Virus	A program or piece of code that is written to deliberately produce an unexpected - usually negative – event, and to reproduce itself without the knowledge of the computer user. Viruses can damage hardware, software, or information.	These days, viruses usually come attached to e-mail messages, although they can also be spread by exchanging disks or downloading files from the Internet.
Worm	A type of malware which spreads itself across a network without user action and distributes copies of itself across computer networks. A worm can use up memory or network bandwidth, causing the computer to stop responding.	Just by being connected to the Internet, if you do not have adequate protection.
Trojan	A computer program that appears to be legitimate but that actually does malicious damage.	By being tricked into opening a file (such as free downloaded software, or an attachment to an e-mail message) which is actually malware.
Spyware	A type of malware which gathers information about the user and reports it back to the developer/distributor of the Spyware.	By installing software with a hidden Spyware component.

Please continue if you want to know more about Spyware…

Spyware is a problem not just because of the invasion of privacy it creates. It also affects the performance of the computer system because it uses both the processor and the bandwidth of the user's Internet connection to carry out its task. It can also allow your computer to be infected by viruses or hacked into via the Internet.

Spyware may do any of a number of things…

Surveillance software tracks activities on a computer. For example, key loggers track every keystroke made.

Advertising spyware ("**adware**") logs information about the computer user, such as e-mail addresses, online buying habits, Web sites visited, passwords and computer configuration. This type of spyware can also modify your browser settings, for example changing your home page to an unwanted – often pornographic - Web site, or displaying unwanted advertisements. Sometimes it will be quite obvious to you that adware has been installed on your computer; in other cases the adware may be silently collecting data without your knowledge.

Avoid adware by…

- Making sure that your computer **cannot automatically download** and install software without your consent. Configure your browser to use a higher security setting. You should then see a prompt every time a program tries to install itself.

- Reading the **license agreement for any software** that you download. Some distributors of adware count on the fact that most users don’t bother to read these agreements.

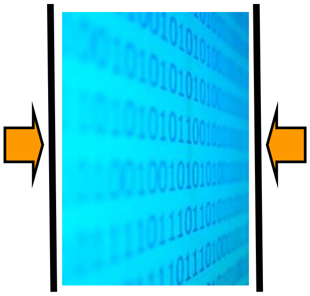
- Using an **anti-adware tool** which monitors your computer for adware, and removes any adware which is found.

Ad-Aware Standard Edition from Lavasoft is a free detection and removal utility for Microsoft® Windows® 98/Me/NT/2000 and XP Home and Professional. http://www.lavasoft.com/

Spybot - Search & Destroy, is a free tool which can detect and remove spyware of different kinds from the computer. http://www.spybot.info/

Annex 4.4.2
Mini-lesson: Compressing and archiving files with the WinZip 9.0 “wizard”

Tools such as WinZip enable you to compress (“zip”) and decompress (“unzip”) files, and to create archives. Many programs can also **encrypt** the compressed archive to prevent access to the information without a password.

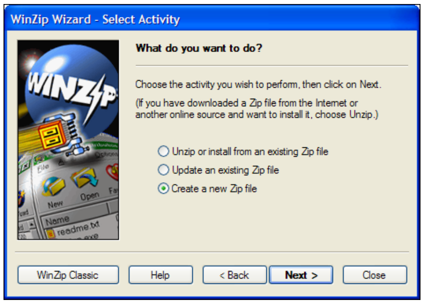


WinZip is one of the most widely used compression tools for the Windows operating system. A free evaluation version can be downloaded from http://www.winzip.com/

The **WinZip wizard** offers a simple interface for unzipping existing files, updating existing zip files, and creating new zip files. (If you wish to make use of more advanced setting options choose the **WinZip Classic interface** when you start the program.

On the next screens, we look at how to create a new zip file.

1) Select **Create a new Zip file** in the **Select Activity** dialogue, and click on **Next**.



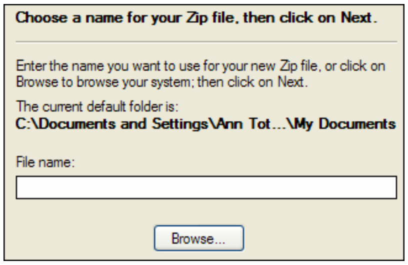
What do you want to do?

Choose the activity you wish to perform, then click on Next.

(If you have downloaded a Zip file from the Internet or another online source and want to install it, choose Unzip.)

○ Unzip or install from an existing Zip file
○ Update an existing Zip file
● Create a new Zip file

2) Name your file, and click on **Next**.



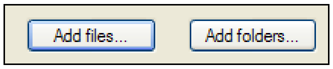
Choose a name for your Zip file, then click on Next.

Enter the name you want to use for your new Zip file, or click on Browse to browse your system; then click on Next.

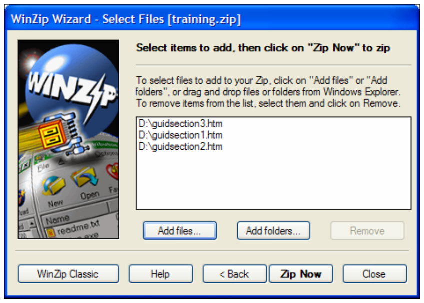
The current default folder is:
C:\Documents and Settings\Ann Tot...\My Documents

File name:

3) Click on **Add files** or **Add folders** to select the files you wish to include in the archive.



4) Select the files to add, and click on **Zip Now**.

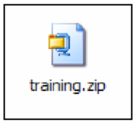

WinZip Wizard - Select Files [training.zip]

Select items to add, then click on "Zip Now" to zip

To select files to add to your Zip, click on "Add files" or "Add folders", or drag and drop files or folders from Windows Explorer. To remove items from the list, select them and click on Remove.

D:\guidsection3.htm
D:\guidsection1.htm
D:\guidsection2.htm

Your zip file is now ready.

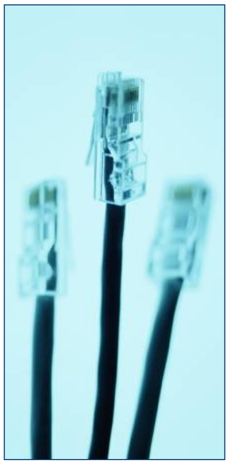


Annex 4.4.3
Mini-lesson: Using passwords

COMPUTERS
If you leave your computer unattended, or if it is stolen, anyone will be able to access all the information it contains. Operating systems such as Windows offer password protection to restrict access to designated users of the particular computer. For example, in Windows XP, you can create a password from **User Accounts** in Control Panel.

Although this offers little protection against people who are seriously determined to steal your information, it is the simplest precaution you can take, and likely to be effective against casual theft.

FILES
Apart from password protecting access to your computer overall, office productivity software such as OpenOffice.org and Microsoft Office generally let you password protect **individual documents** by requiring a password in order to open and/or modify them.



ONLINE SPACES
Passwords can be required to access **online spaces** such as Web sites, discussion boards and wikis, or to modify the information they contain. Think about the online spaces for which you are responsible. Ask yourself:

- Does this space contain any information which should not be open to the public?
- If access restrictions are needed, **to whom** should access be restricted?
- What **levels** of access restriction are required? For example, should only certain groups of people be able to read the information contained in the space, or should everyone be able to read it, but only certain groups of people of individuals be able to modify it?

If you decide that restrictions on access are required, ensure that you or your technical support set up corresponding password protection.

NETWORKS
Passwords should be required for logging on to local area networks (such as those within an organization).

Finally, please take into account following **password tips**…

- Don’t give your password to anyone else.
- Don’t use personal information such as your phone number, mother’s name, or the name of your cat as a password.
- A password should ideally be a random sequence of alphanumeric characters not less than six characters long, using both upper and lower case character. For example: KH92hw.
- Never use sequential passwords (such as the names of days or months)
- Don’t reuse passwords - or at least not within a year or two of their previous usage.
- If you have reason to believe that someone has accessed your system without permission or supervision, change your passwords immediately.
- Never use the same password more than once on the same system.