

**Working towards ECDL
Information and Communication Module
Task 9**

Internet Security

This task sets out information that may be asked in your test. Please note that other questions may be asked that are not mentioned below. Use the search tool and your skills and knowledge gained within this module to discover further the security surrounding the internet.

Understand the terms cookies, cache**What are web cookies?**

Web cookies are simply bits of software placed on your computer when you browse websites. Not all websites have these, but many do, especially the large well-known websites. Websites use cookies so they can track what you are viewing, and although they won't necessarily know you by name (lets hope it never gets to that point), the website will recognize your computer when you come back to visit again.

What good are cookies?

Cookies have some beneficial things. For example, when you log on to certain sites, did you ever notice that when you return again you do not have to sign on the next time? That's because it stored your password and ID on your machine in a cookie. The same holds true when you purchase goods online, you can return later and your goods are still in your shopping cart (in a cookie!).

How do I get rid of cookies?

There is an option in your browser to ask if you want to accept cookies, but that is a real pain because you constantly are clicking buttons saying "no". It makes browsing very difficult when you spend all your time answering "no" to every cookie, since they are all over the net on most websites.

What are cache files? Are these related to cookie files?

Cache files help your browser go faster since it caches the files to be used. These are also left behind on your pc and includes everything, including pictures, sound files, video files, and text that you have browsed.

What is the best way to keep my information private? How do I keep my email from getting spammed?

Most websites today that sell anything online are pretty good about keeping your information confidential (obviously not all of them though!). Many even state this when you are ordering, as there is normally a link saying that they keep information private. You can help limit your information by not filling in information on sites that are NON-ordering sites. For example, you know those sites that want to send you a free magazine by just filling in your information and clicking ok? Many of those sites are giving you free stuff so they can get your information.

If you would like to keep your email from getting spammed, you can do a few things. First, send them a nice email and tell them not to email you again, or most internet email accounts now have blocking features on the email that you can set to block specific emails, or only allow specific emails. This can save you the trouble of even asking someone to stop, just simply shut them off!

Is it safe to store password information on my computer?

I would recommend NOT storing passwords on your computer, mostly because your computer can be stolen, or you could have someone hack your pc online. These are rare situations, but it's not worth the risk of having your passwords taken for banks, brokers, online accounts, and many other personal sites!

Know what a digital certificate is?

There are many definitions of Digital Certificate on the Web. Some of these are:

"A digital certificate is an electronic means of establishing your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticated users can look up other users' public keys".

"Digital Certificates are issued by a Certificate Authority, which verifies the identification of the sender. The certificate is attached to an electronic message, so the recipient knows the sender is really who they claim to be".

"A digital stamp, using encryption technology that certifies where a digital document came from. A certification authority backs up the certificates".

"A Digital Certificate is a digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. A Digital Certificate is a data structure used in a public key system to bind a particular, authenticated individual to a particular public key"

"A digital certificate is a secure electronic identity that certifies the identity of the holder. Issued by a Certification Authority, it typically contains a user's name, public key, and related information. A digital certificate is tamper-proof and cannot be forged, and is signed by the private key of the Certification Authority which issued it".

Know what encryption is and why it is used.

Encryption is a method of hiding data so that it cannot be read by anyone who does not know the key. The key is used to lock and unlock data. To encrypt a data one would perform some mathematical functions on the data and the result of these functions would produce some output that makes the data look like garbage to anyone who doesn't know how to reverse the operations. Encryption can be used to encrypt files that the owner feels are too sensitive for anyone else to read. And now, with the rise of the Internet, encryption is used to encrypt data, like a credit card number, and then send it across the net. This way no one can read, intercept and read the data while it is travelling through the web. The recipient of the data does have to know how to decrypt the information or else the data will look like garbage to the recipient too.

There are two categories of encryption, private key and public key. The major difference is who knows the key. Encryption is an entirely mathematical process applied to the world of computers. The only thing an encryption program will do is take in data, perform some predefined mathematical operations on the data, and then output the result. Decryption is the process of taking the encrypted data that now looks like garbage, and reverse the mathematical functions so that the result is the same data

that originally existed before the encryption process. The "key" is the set of mathematical operations and values that are used to encrypt and decrypt the data.

Encryption and decryption algorithms describe the mathematical operations while key describes the exact process which includes the algorithms and any other random initial values that are used in the algorithms. Lets first look at private key encryption and how it works.

Private Key Encryption

What private key means is that the same method is used to encrypt and decrypt. If someone knows what method was used to encrypt the message then that person can decrypt the message. Thus, the key must be kept private. Only the person sending the data and the person receiving the data should know the key. Private key cryptography, also known as symmetric cryptography since the encryption and decryption processes are just opposites, is an encryption method where the encryption algorithm is known before hand by the sender and the recipient. Accordingly, the two users must communicate beforehand and agree on the algorithm and the key so that the recipient can decode the message. A very simple example of private key cryptology is to take the text that is to be sent across the Internet and use the next letter in the alphabet in place of the original letter. Then send the scrambled text across the Internet. The person receiving the text would have to know how the message he receives is scrambled so that he can unscramble it. Thus, the "key" being used in this example is, 'use the next letter in the alphabet.'

With this key the text, "hi rob" would become, "ij spc". Since the recipient of the message knows the key, that person will take the message he received and take the previous letter in the alphabet. The person would receive the message, "ij spc," and using the previous letter that person would recover, "hi rob." This example is much simpler than the private key encryption algorithms used today, but it illustrates the fact that in private key encryption the encryption and decryption processes are just the reverse of each other

Private key encryption has the benefits of being very fast in that the computer programs that will perform the encryption and decryption will finish executing in a very short amount of time. The more complex the key the longer the process takes. However, even the most complex private keys algorithms can encrypt and decrypt data faster than that of public key cryptology. A disadvantage to private key cryptography is that the key must be communicated before hand. You would have to tell me exactly how you were going to encrypt the messages that you will send to me so that I could recover the

original message later. You could not encrypt this information as I wouldn't know the key yet. In a large organization or over the Internet it is easy for these keys to become compromised because they have communicated, without using encryption, before the actual encryption takes place.

Public Key Encryption

Public key cryptography (asymmetric) was created to eliminate the shortcomings of private key cryptography. The biggest advantage of public key cryptography is that no prior communication needs to take place between the recipient and the sender.

Public key cryptography works like this, everyone has two keys, a public key, which the entire world has access to, and a private key, which only the owner knows. Note that the private key referred to here is completely different than the private key used in private key cryptography. For lack of a better name the secret key in public key cryptography is called a private key. These two "keys" are much different from the "keys" used in private key cryptography. In fact both keys used in public key cryptography are just very large integers, on the order of 300 digits long. With public key cryptography there is only one algorithm that is in use, that algorithm is known as the RSA algorithm. The RSA algorithm is the only algorithm that will be used to encrypt and decrypt data.

The algorithm works by taking in some data, and then using one of the keys which is a large number, and using the key to perform modulo and exponential functions on the data. The result is a message so scrambled that no amount of statistical analysis could break the code. The beauty of RSA is that a message encrypted with a public key can be decrypted with the corresponding private key and a message encrypted with a private key can be decrypted with the corresponding public key. For this reason RSA is known as asymmetric cryptography, different algorithms are used to decrypt and encrypt data. The algorithm is actually just a very complex mathematical identity. Thus, person X can encrypt a message with person Y's public key and only person Y can decrypt the message using his private key, this is the process used to encrypt e-mail. More importantly, if I had a public and private key, and only I know my private key, I could encrypt a message using my private key and everyone could decrypt the message using my public key. If my public key successfully decrypts the message you can be sure that I sent it because the message could have only been created with my private key. The reason it could have only been created with my private key is that my public key was used to decrypt the message. By decrypting the message with my public key you know only my private key created it. This works as long as only I have access to my private key. The process described here is known as a digital signature because by creating a message that only I could have created I am effectively signing the message.

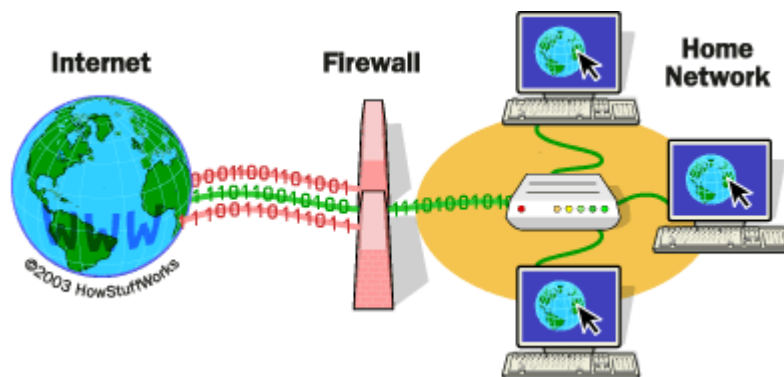
Like private key cryptography the encryption and decryption process must reverse each others actions, but the difference lies in that there are two different numbers and two different algorithms used. One number is the public key and the other number is the private key. These numbers are used in the two different algorithms one to encrypt a message and one to decrypt a message. The important aspect of RSA and public key cryptography is that no prior communication has to take place before a message is sent. If you receive a message encrypted with RSA and your public key you have all the information you need to decrypt the message. RSA does have some disadvantages however, since the numbers used are so large the amount of time it takes to encrypt or decrypt is a lot longer than private key cryptography.

What you should understand now is that there are two methods of encryption, private key and public key, each with its own advantages and disadvantages.

Understand the term firewall.

If you have been using the Internet for any length of time, and especially if you work at a larger company and browse the Web while you are at work, you have probably heard the term firewall used. For example, you often hear people in companies say things like, "I can't use that site because they won't let it through the firewall."

If you have a fast Internet connection into your home (either a DSL connection or a cable modem), you may have found yourself hearing about firewalls for your home network as well. It turns out that a small home network has many of the same security issues that a large corporate network does. You can use a firewall to protect your home network and family from offensive Web sites and potential hackers.



Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why it's called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next.

Be aware of the possibility of receiving unsolicited email (Spam)

If you have created an email account with yahoo, look for the Mail Options (top right hand side of the screen) to read more in depth about Spam mail. Alternatively use the search tool on when connected to the internet.

Be aware of the danger of infecting the computer with a virus by opening and unrecognised mail message. An attachment contained within an unrecognised mail message

One of the ways of a computer becoming infected is by opening unrecognised mail. You will not know that there is a virus attached until it is too late. The best thing to remember is that if you do not recognise the name of the sender or are not expecting any emails is to delete the sender and message immediately without opening it.

One of the latest virus is 'My Doom' which is an email worm which spreads quickly throughout your emails, files, and computer system. The file attachment is often in a ZIP archive format and can have any one of a number of file extensions, including .exe, .pif and .scr.

What is a virus?

A computer virus is a programme designed to alter the way a computer operates, without the knowledge or consent of the user. There are two key aspects of a virus:

- 1 They are self executing. Typically, a virus will attach itself to another programme on your computer, so that it is activated when that programme is used.
- 2 They are self-replicating. Viruses are designed to spread from machine to machine and across networks. To achieve this, a virus will usually copy itself to other programmes on a computer, before executing any intended tasks.

There are a huge number of viruses in existence, carrying varying degrees of risk. Some are extremely malicious, with the ability to delete or damage files and programmes. Others are less destructive, but prove debilitating by jamming resources, causing systems to crash with consequent loss of data.

Some of the most well known viruses are:

- Bugbear
- Klez
- Lovebug
- Melissa
- Bubbleboy
- Code Red

Some viruses will hit as soon as they reach a machine, and signs of infection are immediately obvious. Others can remain hidden until triggered by a future event. It is therefore vital that full and thorough recovery procedures are followed when an infection occurs.

Different types of virus

Although there is a large number of viruses, they fall into three main types:

- Macro viruses use features within standard applications, such as Microsoft Word and Excel to perform unexpected tasks. For example, inserting unwanted phrases or figures
- File viruses normally affect programme files and are usually transferred by disc, file transfer or e-mail attachments
- Boot sector viruses infect parts of your computer that are used when it starts up, typically the floppy disc and the hard disc. In doing so, the very act of starting a PC will activate the virus

You may also have seen the terms worm and trojan horses used in the context of viruses. These are variations on viruses with their own characteristics.

What is a worm?

A worm is a programme that is designed to replicate and spread throughout a computer system. It will usually hide within files (for example, Word documents), and distribute those files through any available network connections.

Worms are often used to drain computer resources such as memory and network access, simply by replicating on a large scale. In addition, worms sometimes delete data and spread rapidly via e-mail.

What is a trojan horse?

A trojan horse is a malicious programme, usually disguised as something useful or desirable. When activated, they can cause loss, damage or even theft of data.

The critical difference between a trojan horse and a virus is that a trojan horse cannot replicate itself. The only way that a trojan horse can spread is if you help it! For example, saving the programme from an e-mail attachment, or downloading it from the Internet.

Just because trojan horse programmes are not self-replicating, it does mean that they are any less destructive than a virus. Some common features of trojan horse programmes include:

- Rounding (carving off small parts of payments from a large number of accounts or transactions)
- Causing payment triggers (causing illicit payments to be activated)
- Making configuration changes
- Distributing security information
- Providing unauthorised access paths (known as backdoors and trapdoors)

What are the characteristics of a virus?

Some of the most common characteristics of a virus are:

- A sudden decline in PC or network performance
- Playing a tune or displaying a message
- Loss of files or data
- Loss of partitions (organisation of disc space)
- Unauthorised release of files, usually via e-mail

Remember that just because you have some signs of a virus, it may not in fact be the case. It might be a virus hoax.

How are viruses transmitted?

Viruses are usually disguised as something else. For example:

- E-mails or e-mail attachments
- Internet downloads
- Internet pages
- Software releases on disc or CD

You are at risk from a computer virus infection if your computer system is used to communicate with others, be it via a network, the Internet or e-mail. Given that these are now the main reasons that we are using computers, the risks are very real.