IT-security

Faculty of Agricultural Sciences

Why is IT-security important to me?

Most of us are not usually aware of the importance of IT security until something goes wrong. You might lose what you have been working on all day or your computer may be attacked by a virus when you are most busy. With a little care you can save yourself a lot of frustration and wasted time. This folder will give you some basic but sound advice that can be used in your daily work with a computer.

The most useful tool in securing your computer and keeping important documents safe is your own common sense – *you do not need to be an expert!*

Password

It is very important that you choose a good password, as it is the first line of defence. It is therefore not a good idea to use a common word or name. The programs used to break passwords contain all words found in the dictionary as well as most known passwords. Therefore, your password ought to be *minimum* 8 characters - consisting of numbers, upper and lower case letters as well as special characters. It is important that you are able to remember the chosen password without having to write it down. Your password is personal and should therefore not be given out to others.

Lock your computer

When you leave your computer it is a good idea to lock it or use a screen saver with a password. If your computer is unlocked it is possible for anyone to read any data that you have access to, e.g. your e-mail or the internal DJF network.

E-mail

All employees at DJF receive a DJF e-mail account. When you send e-mails from your DJF account it is important to remember that you are a representative of DJF, as it corresponds to sending a letter on official DJF stationery, so therefore you need to carefully consider the use of your account.

Attached files in an e-mail

Attached files in an e-mail might contain spyware and viruses, so therefore you always need to be very careful when you receive e-mails with attached files, this should include files sent by known as well as unknown senders. You should never open executable files (files ending with *.exe, .bat, .pif, .scr* and *.com*). Furthermore, you need to be cautious of attached Word files (*.doc*) and Excel files (*.xls*) received from unknown sources. These files may contain viruses and spyware (in the macros).

Virus

If you suspect that your computer is infected with a virus or if you have opened files that you are unsure of, you need to contact your local IT technician or call the IT unit (1785). It is extremely important that you do this immediately as a virus can spread very quickly throughout the entire network, but prompt action can limit the damage that may occur.

Spam

At DJF we have a spam filter (Barracuda) installed to catch most of the spam sent to the network. Unfortunately it cannot catch all spam mails. The spam senders are constantly finding new ways of creating spam and the filter needs time to learn these methods before it can catch the latest varieties of spam. On a normal day DJF receives approximately 120,000 e-mails, of which around 110,000 are categorised by the filter as spam.

Why do I receive spam?

The spam market is incredibly large and somewhere in the region of 61 billion spam mails are sent around the world every day. Most of the e-mail addresses are picked up from web pages where you have entered your own e-mail address. Thus, it is important to consider very carefully where and to whom you submit your e-mail address. You should never answer a spam mail because then the sender knows that the e-mail address is used and they will continue to send spam.

Phishing

Phishing is a webpage/e-mail sent to you pretending to be from your bank, telephone company or any other place that you might use your credit card or bank account details. Always think twice when you receive e-mails asking for personal information or containing invoices. If an *.exe* file is attached, do not open it as it might take all the information from your computer and send it to a hacker.

P2P, movies and music from the internet

On the DJF network file share programs (bittorrent, dc++, edonkey, etc.) are not allowed, as it is illegal to download movies, music and programs from the internet without paying for them first. DJF could face large claims for compensation if downloads take place from our network. The firewall log is frequently checked to ensure that no one uses these programs. If you do use a file sharing program, your access to the internet will be blocked automatically until the programs are deleted. During this period you will only have access to the internal IT servers (files and e-mail).

Network security

When you work on the internet you may meet pages that ask you to install certain programs (often in the shape of virus scans, etc.). This might be spyware that collects data concerning what you do on the internet and could send personal information, e.g. details of your bank account, etc. on to an unknown party. Therefore you need to be very careful when you download or install anything from the internet. It is important to consider if it is necessary for you to download the program and whether you can trust the web page that you are downloading from. When in doubt on whether to download or if you think you computer may have been infected with spyware, you should immediately contact your IT technician.

Who can see what you do on the internet?

DJF does not monitor what you do on the network, but DJF logs all network traffic as a necessary precaution to help possible trouble shooting. In this connection it is possible to see the current network traffic. DJF reserves the right to monitor and examine your activities and saved data on the DJF IT systems. Such an investigation is always made in confidence by special employees and to your prior knowledge. Unauthorised use of the network is regarded as a problem with cooperation and management and will be treated as such – contraventions of the law will be reported to the authorities.

The DJF network

Basically you are not allowed to connect an external/private laptop to the DJF network. If - for some reason - you need to do so, the computer must first be scrutinised by an IT technician as it might be infected with a virus, spyware or hacking programs that can damage the entire DJF network. External/private laptops may only be connected to the DJF-guest wireless network, as this network is separate from the DJF network.

Who owns the data?

If no prior agreement has been made in writing, DJF owns all data located on the DJF network and computers.

Data on portable media

You must always consider very carefully what you are doing when you transfer data to portable media (laptops, memory sticks, CD/DVD or external hard disc) as the media could become lost or stolen. Never insert a memory stick or CD/DVD that you are unsure of into a DJF computer, as it may, without your knowledge, install hacker programs when you inserted the media. If you find items like this, hand them in to your local IT technician.

Laptops

On all new laptops it is possible to install a password directly on the hard disc (ata-password) to ensure that the hard disc cannot be removed and placed directly into another computer. An ata-password is an extra code that you need to type in as soon as the computer is turned on in order to activate Windows. Having this password on the hard disc is a good idea, especially if you take your laptop on a business trip. An ata-password ensures that it is not immediately possible to access data from the laptop if it gets lost or stolen. Your local IT technician can help if you need an ata-password installed.

How to avoid losing data

In order to avoid losing data it is a good idea to save your data on the network and not on a local drive, as security backups are taken from the network on a daily basis. It is also a good idea to frequently save what you are working on (it can be done automatically in most Office programs). If you do lose data, please contact your local IT technician or the IT unit.

Good advice on security:

1. Use your common sense
2. Always use a safe password
3. Never give out your password to anyone
4. Be careful when incoming mails have attached files
5. Always make sure that your computer has reliable antivirus programs installed
6. Think about what you do on the internet and be careful of what you download
7. Think twice before giving your e-mail address or other personal information to other people
8. Think about what you transfer to portable media
9. Save your work frequently
10. Remember to back up your files

You can read more about what you can and cannot do on the DJF network and IT-infrastructure on http://djf-intranet/it/index.html

If you have any questions regarding this folder or regarding IT-security in general, you can call or e-mail the IT-unit on telephone: 1785 or e-mail: >1785

René Sørensen and Karina Christensen
Revised 29 July 2008