

0. If you read nothing else, read this!



If you have absolutely no time or interest to read or even browse through this manual, we have collected the most essential matters about the University of Turku computing services on this page. Merely reading these will save you from a lot of mistakes and frustration with the University computer systems.

The username and passwords you have received are personal.

It is absolutely forbidden to give your passwords to anyone else. This will result in immediate loss of user permit. More information in chapter 2.2

Your passwords expire.

Most passwords are good for 90 days, and if they are not changed, they will stop working. Even the passwords that don't expire should be changed every once in a while. More information in chapter 2.2.3

You are responsible for your own computer.

If you have your own computer connected to the University network (a home computer or a notebook), make sure its virus protection and firewall are up-to-date. Keep its operating system updated (in Windows, use Windows Update regularly) or its security holes can be used to break into the system. See chapter 4

Remember that e-mail sender information can be forged.

Do not assume that all mail seemingly coming from people you know is genuine. You should regard all mail with some amount of suspicion, and remember that attachment files are always a security risk. Take special care with attachments sent unexpectedly from acquaintances or "administration"; these are almost certainly viruses. See chapter 5.2

If you need correct information, see the Computing Centre Web pages (or other official and trustworthy sites). Do not believe in rumors spread by e-mail, scare attempts by shifty Web pages, or your all-knowing pal.

Terms and conditions of use apply to you even if you haven't read them. There are a lot of decrees and conditions concerning the use of computer systems, and not knowing them is not a valid excuse for not abiding by them. It's best to read the Terms and Conditions at <http://www.cc.utu.fi/>, especially if in doubt on what you can and cannot do.

0. If you read nothing else, read this!	3
1. Welcome to the University of Turku Computer Services	6
1.1. Computer Services and the Computing Centre.....	6
1.2. Updates and Additional Information.....	6
1.3. Computer Courses.....	7
2. User Accounts, Passwords, Rules	7
2.1. User Account.....	7
2.2. Passwords.....	8
2.2.1. Why Is My Password so Secret?.....	8
2.2.2. How Do I Keep My Password Secret?.....	8
2.2.3. How Often Should I Change My Password?.....	9
2.2.4. What Is A Good Password Like?.....	9
2.3. Microcomputer Network Password.....	9
2.4. E-mail Password.....	9
3. University Workstations	10
3.1. Security of a University Workstation.....	10
3.2. Workstations for Students: Labs, Libraries, Public Terminals.....	10
3.2.1. Computer Labs of Departments and Faculties.....	11
3.2.2. The Computer Lab of the Computing Centre.....	11
3.2.3. Public Terminals.....	11
3.3. Logging On and Changing the (Microcomputer Network) Password.....	12
3.3.1. Changing the Microcomputer Network Password.....	12
3.4. Printing.....	13
4. Private computers	13
4.1. Security of a Private Computer.....	13
4.1.1. Ground Rules in Security.....	14
4.1.2. Windows Security.....	14
4.1.3. Macintosh Security.....	14
4.1.4. Linux Security.....	15
4.2. SparkNet: Public and Wireless Network.....	15
4.2.1. Connecting Your Computer to SparkNet.....	15
4.2.2. User Rights and Logging On.....	16
4.3. Software Distribution for Private Workstations.....	16
5. E-mail	16
5.1. E-mail Etiquette.....	16
5.2. E-mail Security.....	17
5.2.1. Junk Mail Prevention.....	17
5.2.2. E-mail Viruses.....	17
5.2.3. Hoax Warnings, Scarygrams and Phishing Attempts.....	18
5.3. E-mail Programs.....	18
5.3.1. Utu Webmail.....	19
5.3.2. Mozilla Thunderbird.....	19
5.3.3. Mobile Devices and E-mail.....	19
5.4. Space Restrictions in E-mail.....	19
5.5. Additional Functionality.....	20
5.6. Mailing Lists.....	20
6. Data Storage Services	20
6.1. Personal Home directory: "Oma verkkokansio".....	21
6.2. Personal WWW folder.....	21
6.3. Other network drives.....	21

7. Other Services	21
7.1. Wenti.....	21
7.2. Calendar.....	22
7.3. IRC service	22
7.4. Unix	22
7.5. Library Services.....	22
7.6. eWert Online Newsletter.....	22
7.7. Et cetera	22
8. Connecting from Outside the University	22
8.1. Modems	22
8.2. The Student Village Network	22
8.3. The College ADSL	23
8.4. Remote Connections to University Services	23
8.5. Connections with Mobile Devices.....	23
9. User Account Regulations: Students	24

1. Welcome to the University of Turku Computer Services



This manual is intended as an introduction for new students as well as a reference for experienced ones. It is available at the Computing Centre, 4th floor of the Educarium Building.

The text for this manual has been composed by Dare Talvitie, and the pictures are courtesy of Suvi Ylioja.

This manual assumes the user already knows the basics about using computers, and therefore concentrates on the use of computers in the Turku University environment. The basics we don't cover include how to turn the computer on, how to open or close programs, the basic use of Windows or other operating systems etc. Manuals and courses on these topics are available elsewhere; see chapter 1.3

Feedback on this manual, as well as questions about the University computer services can be sent by e-mail to pulmalinja@utu.fi

1.1. Computer Services and the Computing Centre

Basic computer services at the University are provided by the Computing Centre. These basic services include maintaining the network and its services, administering and developing supported systems and programs, and providing instructions and support with the services.

For the most part computer services are free for students. The University network, e-mail, disk space and other services described here and on our Web pages are available to students based on their membership in the university. Some specific services (home network connection, keys to computer labs) have a price, but there is always a notification about these. In practice the university systems can be used freely.

As a member in the university you also have an obligation to be responsible in your use of the services, with consideration towards other users of the services.

1.2. Updates and Additional Information



Computer services provided by the university are constantly evolving, and much of the information in this manual will probably be obsolete before the next update gets made. This manual doesn't even attempt to contain all the relevant information about the computer services. The most up-to date information can be found on the Web pages of the Computing Centre, a

<http://www.cc.utu.fi/en>

The links on this page should provide more information on services offered, as well as help you with most problems you're likely to encounter. When you run into a problem you don't

know how to solve, the Computing Centre Web pages are a good place to look for a solution.

Due to the ever-changing nature of the World Wide Web, no exact links to help pages are usually provided. Whenever this manual refers you to seek more information on the Web, the aforementioned front page is the best place to start

If the instructions on the Web are not sufficient, more information relating to the University computers, software or network connection is available at the Help Desk. You can call us (+358 2 333 6000) or e-mail us at helpdesk@utu.fi.

You can naturally also visit us. The Help Desk lies on the 4th floor of the Educarium building, and is open weekdays from 8am to 4pm.

1.3. Computer Courses

The Computing Centre does not teach courses. Most of the courses intended for students are given by the Department of Information Technology. More information can be found in the Study Guide for the Faculty of Mathematics and Natural Sciences, on the Information Technology Web pages, or on the department bulletin boards. Some curricula have their own mandatory computer classes. Usually student organizations have also given new students e-mail classes and the like.

2. User Accounts, Passwords, Rules

2.1. User Account

A user account is a personal permit to use the computer resources of the university. It is required for using any university computer services.

For degree students, a user account is generated automatically and the username and password are sent to her home address when enrolling. For exchange students, a user account must be applied for by filling in a form at Student Services. The form, which is also available on the Computing Centre Web pages, must be returned to Computing Centre in person.

The user account is **personal**, and remains valid as long as the student is attending the University.

All matters concerning user accounts are handled by the Help Desk, in the fourth floor of the Educarium Building, on weekdays from 8 AM to 4 PM. Be prepared to present valid identification (e.g. a passport) when dealing with matters concerning user ids and passwords.

2.2. Passwords

A password is required to use the user account. Your user account is your home address and your password is the front door key. Your passwords are strictly personal: the conditions of

use do not give you the right to give out your password to anyone else.

This manual and other instructions refer to two passwords: the *e-mail password*, and the *microcomputer network password*. Most services (e-mail, Wentti, SparkNet) are accessed with the e-mail password. The microcomputer network password is used to log on to Utu domain, in unix connections and some remote access applications.



2.2.1. Why Is My Password so Secret?

The user account and its password are a powerful tool, making it possible to wreak a lot of destruction in the computer the account is in. In addition to this, the username-password combination provides a way for a cracker to break in deeper into the university computer system.

The user is responsible for his account in the network and on the university servers, therefore he is also liable for any damages and criminal charges caused by the misuse of the account. Some services (eg. ordering the College ADSL) are , which are billed by user name.

2.2.2. How Do I Keep My Password Secret?

The most important means of keeping your password secure is changing it regularly. Even a good password can be cracked, but changing it reduces the amount of time the cracker has to misuse the account.

Every user changes his own passwords personally, as the user account is strictly personal. You can ask for help in changing your password, but even then the person assisting you must not be told your old or new password.

Another important security measure is to take good care of your password. If you don't remember it without writing it down, make sure you keep the note with your password on it in your wallet, purse, cellular phone etc. all the time do not leave it in your desk drawer, or on a Post-It note attached to your screen etc lest a random bypasser find it.

It's equally important not to use the same password in more than one system. For instance, if you have an account both at the University and in Hotmail, whatever you do do not use the same password for both!

Some network connections are easy to eavesdrop on. This applies especially to telnet connections and unencrypted www and e-mail connections. You must not use the University passwords in connections such as these. All the services provided by the University use encrypted connections and are difficult to eavesdrop on.

2.2.3. How Often Should I Change My Password?

According to the user account application, you must change your password once every three months.

Most passwords expire in 90 days and therefore have to be changed with intervals of no more than 90 days. If a password expires, it can no longer be used to log on normally. An expired microcomputer network password has to be changed immediately after logging on.

2.2.4. What Is A Good Password Like?

There are several ways to make up a good password. The goal is to create a word that's easy to remember but hard for others to guess. In theory a password should be complete gibberish. However a password is easier to remember if it's pronounceable.

A bad password is easy for an outsider to guess. Your name (even reversed), the name of your spouse, children, pet, birth dates are all relatively easy to find out and therefore dangerous to use. Equally bad are words commonly associated with passwords, such as "password" or "secret".

In order to make program-based cracking impossible, the password must not be a word found in any dictionary, in any language. In theory, a password must not be any word in its basic form. Passwords based on calendar names are easiest to guess.

Replacing a letter or a part of a word with a number or a special character that resembles it, or adding a number as a first or last character to a word in its base form doesn't add to secrecy either. Don't choose, for instance, as a password any of the following: "Orch1d", "5imple" or "1secret2"

2.3. Microcomputer Network Password

The microcomputer network password is used to log on to utu domain. It is not possible to use Windows 2000 or XP computers without logging in with a password. A microcomputer network password has to be changed at least every 90 days or it will stop working. The password is changed either at a University computer, or on a Web page.

2.4. E-mail Password

The e-mail password is used in e-mail programs, as well as the Web based services requiring authentication (the University Intranet or Wentti). It is gradually becoming a general "service password" used to access other services than e-mail. It has to be at least 8 characters in length, but all characters except special characters are allowed.

Previously the e-mail password did not expire. However, a 90-day expiration period will probably be set at some point.

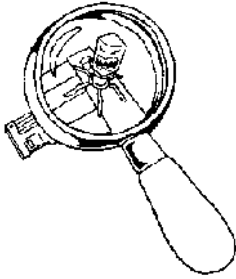
The e-mail password is changed either through Webmail, on a Web page or in the unix.utu.fi mainframe.

3. University Workstations

This chapter discusses computers provided by the University - e.g. computer labs and public terminals. On using your own computers at the University, see chapter 4

3.1. Security of a University Workstation

Microcomputers are susceptible to a wide variety of security hazards. However computers of the University have been made reasonably secure to use. Windows 2000/XP computers connected to the University network and logging on to the Utu domain receive crucial security updates automatically. All a user has to do is restart the computer when prompted.



Every workstation in public use has the F-Secure Anti-Virus program installed. It is automatically updated as well. In theory it should warn the user whenever he tries to run a hazardous program.

However, new viruses appear all the time, and the anti-virus program might not always keep up with them. Therefore a Windows user needs to remember, that any file from an unknown source is a potential virus. In addition, one should keep in mind that a file sent by e-mail is always from an unknown source, since forging an e-mail address is trivial to do. One should not believe that it's safe to open any files since an anti-virus program would prevent dangerous files from opening.

3.2. Workstations for Students: Labs, Libraries, Public Terminals

The University provides public workstations for students. They are available in libraries or computer labs, or as public terminals. Library computers or public terminals are best suited for quick stints in the Net, or for checking your e-mail. Computer labs are suitable for longer stretches of work.

When working on computers in public use, you must save your own work in your personal disk space, a floppy disk, or a USB memory stick. It is not possible to save your files on a hard disk on most of these computers, and it's impossible to use memory sticks or floppies on public terminals . Large documents are saved in your home directory ("Oma verkkokansio").

It's always a good idea to keep up-to-date backups of all your data on a floppy, a memory stick or a network drive. Floppies by themselves are not a reliable backup media. Memory sticks are not quite as susceptible to getting destroyed as floppies, but they too get lost or damaged regularly.

3.2.1. Computer Labs of Departments and Faculties

Several departments and faculties provide computers or computer labs for common use. Usually access to these services is limited to students majoring in the subject taught by the department, or is gained via a user-specific code key. These labs feature the most commonly used programs, as well as special applications determined by the department or faculty. For more information, contact the person responsible for the lab computer support in your department.

3.2.2. The Computer Lab of the Computing Centre

The Computing Centre has a computer lab open to all students. It's situated on the third floor of the new building, and is open 24/7.

Access to the lab requires a magnetic key, which is available for a price of 15 €. You get back 10 € when you return the key. You can purchase the key at the Help Desk. Keys are only sold to students, and anyone wishing to obtain one needs to present a valid photo ID.

Every use of the magnetic key is registered. The register is used eg. in larceny investigations concerning the lab, so don't let anybody in with your own key! Everybody entering the lab must use their own magnetic key, even if the door remains open.



Computers in the lab have Windows XP Professional as their operating system. The lab features the most commonly used programs (Microsoft Office XP, a WWW-browser, a terminal emulation program (SSH), Adobe Acrobat Reader etc). The lab also provides a scanner and a b&w laser printer, to be used for printing related to studies. The amount of printouts is monitored.

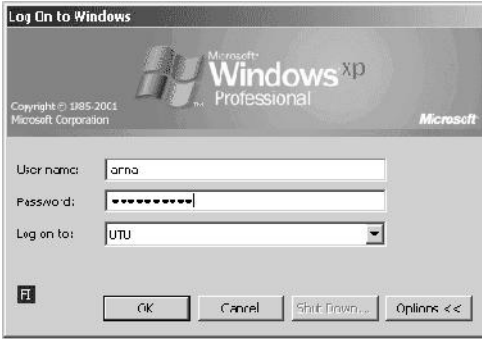
Tech support for the lab is provided by helpdesk@utu.fi (tel. 6000). **Installing new programs on the computers without permission is not allowed. Neither is playing computer games.**

3.2.3. Public Terminals

Scattered around the common areas of the University there are public computers of the UtuKäyPä system. They are intended for e-mail and quick web surfing.

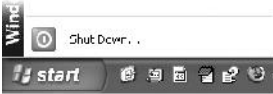
The UtuKäyPä computers require you to log in using your username and microcomputer network password. The user settings are not saved, so you should not save any files you wish to keep on the desktop. Any CD- or floppy drives in the computer are not enabled. Remember to log off when leaving the terminal.

3.3. Logging On and Changing the (Microcomputer Network) Password



Logging on to a Windows 2000/XP computer starts with a login window.

Logging on requires a user name, microcomputer network password, and the domain UTU. (You can also log on by entering username@utu.fi as your user name; the password is the same, but you don't need to enter anything at **Log on to:**)



When you stop using the computer you have to log off. To log off, select **Start -> Shut Down -> Log off** (in Windows XP, merely **Start -> Log off**)

3.3.1. Changing the Microcomputer Network Password



In Windows 2000/XP you change the microcomputer network password by pressing **Ctrl-Alt-Delete** after logging in. You then get the Windows Security window.

Select Change Password.



At Old Password enter your old microcomputer network password. At New Password and Confirm New Password enter a new microcomputer network password. Click OK when done.

It is also possible to change your microcomputer network password on a Web page.

3.4. Printing

You can print documents relating to your studies on University printers. Other printing is not allowed. This is a restriction based not just on amount of paper available; ink consumption and available printer capacity are also factors. Therefore, bringing your own paper does not entitle you to print documents not relating to your studies.

When printing, use common sense, and remember that you do not need hard copies of everything. Even study-related printing is limited to reasonable amounts. When the print quota is reached, printing will no longer be possible for that user. More exact information on these restrictions is available on our Web pages.

4. Private computers

It is also possible to connect your own computer to the University network, both on campus and at home.

Computers owned by students are not supported by the Computing Centre. Our resources to help you with problems with your own computers are very limited. We provide no support at all for software-related problems. The user is responsible for her computer. If the computer causes a hazard or a disturbance for the network, its connection can be closed.

More information on home connections is available in chapter 8.

4.1. Security of a Private Computer

Microcomputers are susceptible to a wide variety of security hazards. The term 'virus' is widely used to refer to any malicious program ('malware') that resides in the computer without the consent or knowledge of the user, and causes trouble. This category includes worms spreading from computer to computer, trojans collecting passwords, backdoor programs that allow crackers to enter the computer, as well as many others. Their propagation is made easier by security holes in programs and operating systems.

Securing a workstation is both the user's and Computing Centre's responsibility. The Computing Centre strives to keep the University network secure and usable, but a privately owned computer is the owner's responsibility. Therefore the user of the computer must also take steps to keep the computer secure. Fortunately this is not particularly difficult. If a computer is determined to be infected by a malicious program, or to have a security hole, the Computing Centre has to close its network connection in order to protect the computer as well as the rest of the network. The computer can be reconnected only after it has been cleaned and all security holes patched.

Please note! The instructions in this chapter are merely suggestive. They are by no means sufficient for home or personal computers that do not get automatic updates or support from the University. Also, they only provide the very basics of security information.

4.1.1 Ground Rules in Security

The following table explains the two basic ways that compromise the security of a micro-computer, as well as some means to protect yourself from them. The defense includes actions the user can take, software that should be installed, and centralized security measures of the administrators.

Even these measures do not provide complete security. New security holes are discovered constantly, and programs that exploit them are sometimes a lot faster than their countermeasures. A new virus might spread to thousands of machines before the first anti-virus program learns to recognize it.

Security threat	Centralized defence (by administrators)	Software defence (on the microcomputer)	User defence
User runs a malicious program (e.g. opens an attachment with a virus)	Virus shield on the email server which tries to intercept most known viruses that are sent by email	Anti-virus software (F-Secure Client Security), to prevent malicious programs from being run	Suspicion towards all files that are opened. Keeping the anti-virus software up-to-date
System has a security hole (e.g. an unpatched Windows 2000/XP) and an external attacker uses it to enter the system	University firewall that aims to stop all attacks from outside the University network	Personal firewall software (F-Secure Anti-Virus Client Security), to prevent unwanted connections to the computer	Regularly updating the operating system and software

4.1.2. Windows security

It is possible to get an anti-virus and a firewall program through the computing centre, and both should be installed. The F-Secure Anti-Virus Client Security serves as both anti-virus and firewall software. Students and personnel can install it on their own computers for free. The easiest way to get the software is by purchasing a TY-Koti-CD from the Help Desk (cost 5€). It can also be downloaded from the Computing Centre's Web pages at no cost. F-Secure Anti-Virus Client Security can update itself as long as the computer has some kind of a network connection.

Home computers do not get automatic operating system updates through the Computing Centre, so the user must look after the operating system updates by herself. When a new computer is introduced, its operating system must be updated before the computer is connected to the network, or it must have a firewall stopping all external traffic enabled. Otherwise the computer will probably get its first virus in less than a minute, and the Computing Centre will have to close its network connection.

4.1.3. Macintosh security

Generally Macintosh computers are more secure than Windows computers. No malicious

programs designed for Windows will affect them, and there is hardly any malicious software written specifically for Macs. However, this situation may change in the future. Also, nothing can secure a system from files run by users themselves.

A computer running Mac OS X normally gets system updates automatically from Apple as long as it is connected to the network. It will only ask the user the permission to install. These updates should definitely be installed. Along with basic caution, keeping the operating system up-to-date seems to be enough to keep a Mac secure.

There is no anti-virus program available for the Macintosh through the University. A firewall program is included in Mac OS X, and it should be enabled especially outside the University network.

4.1.4. Linux security

Current Linux distributions are fairly secure right after installation. There are not many malicious programs designed for Linux, and mostly you can secure yourself merely by making sure you update your software regularly. Windows worms and viruses do not affect Linux computers.

Most of Linux malware consists of worms spreading over the network. Therefore the firewall included with the distribution should be enabled, and only services that are actually needed should be started. If a computer is accessed remotely over ssh, for instance, the user should take care to observe good password protocol and prevent direct remote access for the root account. Otherwise normal caution is enough to keep you secure.

4.2. SparkNet: Public and Wireless Network

SparkNet is the public network of Turku Science Park, which includes the University. You can use it to connect your notebook to the University network, either wirelessly or by public network sockets. It is operational around the University and other SparkNet partners. The coverage is nowhere near perfect in the campus area, but it increases all the time.

More information on SparkNet can be found at <http://www.sparknet.fi/>

4.2.1. Connecting Your Computer to SparkNet

If you have a suitable wireless network adapter in your notebook, you can use SparkNet just by taking your laptop close to an access point. Most wireless network solutions automatically locate any suitable access points within about 20 metres. Usually proximity of an access point is indicated by a sticker such as this:

Tällä alueella toimii langaton Internet-yhteys



If your notebook does not have wireless access, you can use a network cable to connect to SparkNet. Scattered around the campus there are SparkNet sockets you can use to connect your notebook to the University network. The amount of these sockets is constantly growing, so a complete list of their

locations is not given here. These sockets are identifiable by the yellow SparkNet sticker.

4.2.2. User Rights and Logging On

User account at the University also entitles you to use SparkNet. When a laptop is connected to the public network, either wirelessly or with a cable, it will first only let the computer access a logon page. The page is first used to select a connection provider - with the University users this is "Turun yliopisto" regardless of where you are. After this you will enter a page asking for your username and e-mail password. Only after entering them you will be able to connect to other pages or use other network services.

4.3. Software Distribution for Private Workstations

Some software is available for students' private computers through the University. Mainly this means the F-Secure anti-virus and firewall, which are available at no cost. In addition some software is available for a license fee, such as SPSS.

Microsoft applications or operating systems are not available to students through the University. These programs must be obtained from a retailer

5. E-mail

The University of Turku provides e-mail service for all of its students and staff. An e-mail address is automatically created for every user. The e-mail addresses are of the form username@utu.fi. A full-name address is also available. Because people sometimes have identical names, you should not automatically trust that an address by firstname.lastname@utu.fi belongs to the person you assume.

5.1. E-mail etiquette

When using e-mail, a couple of good practices should be adhered to. Messages should be given a subject, sent as plain text (not as HTML), and it's impolite to SHOUT USING CAPITAL LETTERS. More info on how to behave can be found on our Web pages. Some things are strictly forbidden. At the top of this list are all kinds of chain letters, which serve no purpose other than consume disk space and clog the e-mail system. If somebody is caught sending a chain letter, his account is closed immediately, to be re-opened only after sanctions determined by the seriousness of the offense.

Several e-mail messages warning of various viruses or other threats are also circulating through the Net. They have no basis in reality and exist only to clutter everybody's mailbox. They are a kind of chain letter, so don't comply with these instructions and especially don't send them onward. If you want further confirmation on the warning being a hoax, you can find it on e.g. the web sites of anti-virus vendors.

Other inappropriate mailing includes advertising, messages that insult the recipient's religion, race etc., or messages sent only to annoy the recipient. They are not strictly forbidden,

but sending them is contrary to good manners.

5.2. E-mail security

Current legislation sees e-mail equal with ordinary "snail" mail. Your mailbox is therefore protected by letter privacy laws. Despite this, you should not count on complete privacy concerning your e-mail since eavesdropping on the network is unfortunately possible. Sending confidential information by e-mail is not recommended.

Unfortunately, forging e-mail addresses is possible and even easy, so one should not always believe the apparent sender is the actual one. Even an attempt at forgery results in closing the user account for quite a long period, if the culprit is a user at the university. On the other hand, a familiar address is not sufficient guarantee of the authenticity of the message. Viruses often spread using forged e-mail addresses.

When sending e-mail, you should first use other means to make sure you're reaching the right person, just like with regular mail.

5.2.1. Junk Mail Prevention

The university employs a centralized junk mail blocking system. Messages suspected of being junk are tagged with "PMX" and a percentage value in the Subject line. However, no filtering is perfect, and some spam always gets through. You shouldn't complain to the Computing Centre if you still get some spam; we know that some will always slip through the controls. You should never reply to junk mail, because this will only result in more spam.



The sender address of a spam message is often forged. It's possible, for instance, to get spam from administrator@utu.fi or from an address you recognize, but the sender has nothing whatsoever to do with the university or your friend.

Spammers collect e-mail addresses from all possible sources - news postings, web pages or even by trying every possible combination of characters as an e-mail address to a known domain with the intention of finding a functioning e-mail address. It is inefficient and pointless to try and disguise your e-mail address to confuse spammers (eg. firstname.lastname@utu.fi.nospam) even when writing news articles. **Forging your address when sending e-mail is forbidden in the University of Turku.**

5.2.2. E-mail viruses

The only way to get a virus from an e-mail is by opening an attachment file. The virus spreads when the attachment is opened, so it is always safe to read just the text of the message. (Some older versions of Outlook or Outlook Express are a notable exception to this, as they automatically run certain types of file attachments. Using these programs is neither

supported nor recommended.) The Computing Centre recommends using Mozilla Thunderbird as a secure e-mail program.

Some viruses sent by e-mail are disguised to look like security updates or "notes from administrators". One should bear in mind that neither the Computing Centre nor software manufacturers send updates by e-mail.

The University has virus protection on the e-mail server. It should automatically detect and remove most viruses that are sent by e-mail, so that they won't even show to the user. It's best not to blindly trust this measure, however, and keep on regarding file attachments with some suspicion.

5.2.3. Hoax Warnings, Scarygrams and Phishing Attempts

There are numerous messages in circulation that only attempt to fool the recipient into something. A fraudster might attempt to find out your password, the codes to your Internet bank or just get you to do some harm to your computer. Junk mail control stops most of these messages, but not all of them.

e-mail phishing and fraud is becoming more common as well as causing more harm. Practically the only way to keep safe is by being vigilant and suspicious towards requests sent by e-mail. It's important to keep in mind that

forging e-mail addresses is trivial, so just because the sender address seems familiar or official is no guarantee that the message is genuine

neither the University administration, nor most other legal services will ever ask you to send your password or code numbers anywhere by e-mail, or give a suggestion for a new password over e-mail

there are many wild e-mail rumors circulating, but most of these are not worth believing. If you are unsure about something, you should confirm things from a Web page you trust. Do not believe in vague messages sent by e-mail, or your know-it-all friend.

5.3. E-mail programs

The Computing Centre supports the the WWW based Utu Webmail, and in personal workstations, Mozilla Thunderbird over an IMAP connection. All other e-mail programs are unsupported by the Computing Centre, and users wishing to use them are on their own when they run into a problem.

The recommended programs read mail folders on the mail server without transferring them anywhere. This is a handy feature in a shared environment, as the mail can be read at any computer, the mail folder is always the same and the mail doesn't get relocated just because you read it.

To put this briefly:

If you have a computer used only by you, the recommended e-mail program is Mozilla Thunderbird.

If you access your e-mail from computers in public use, or share a computer with someone else, the recommended e-mail program is Utu Webmail.

If you use a mobile device (a net-capable phone, a pocket computer etc) the recommended e-mail program is the one that comes with the mobile.

5.3.1. Utu Webmail

The University has a working WWW based e-mail client again. It is probably the simplest way to read mail. You can use Utu Webmail from any computer connected to the Internet anywhere in the world. To log in to Webmail, use your own username and e-mail password. The address for Utu Webmail is <https://webmail.utu.fi>
There are two versions of Webmail: Sun Java Messenger Express and SquirrelMail. The latter has better functionality with older browsers. Both can be accessed through the address given above.

Webmail is the best program for users who read their mail from whatever computer happens to be around. If you have a personal computer, Webmail is unnecessarily clumsy and slow, and using Mozilla Thunderbird is recommended.

Webmail is not recommended for use in mobile devices or over a slow network connection (GPRS or a modem connection), because Webmail gets all its components over the network and therefore consumes a lot of bandwidth. Over a slow connection it is always preferable to use an e-mail program loaded on the device (Mozilla Thunderbird, program installed on the mobile device etc).

5.3.2. Mozilla Thunderbird

Mozilla Thunderbird is well suitable for users with their own computers. It uses the IMAP protocol to read e-mail folders directly from the server. It does not save e-mail on the micro-computer by default, but it can be configured for offline use eg. in notebooks. More information on Thunderbird can be found in the Computing Centre's Web pages.

5.3.3. Mobile Devices and e-mail

It is possible to read University mail on several mobile devices. A common problem for these is that the mobile devices are not capable of making a secure connection, or recognizing the University security certificate. In this case you can read your e-mail, but the connection is not secure. Mobile devices use general e-mail settings given on our Web pages; more exact information for some devices can also be found there.

5.4. Space Restrictions in e-mail

Every user has a 100 megabytes of space reserved for their e-mail. When this space is exceeded, you will get a notice saying "Mailbox is full" upon accessing your mail, and no

new mail can be delivered. Messages sent to a full mailbox are returned to sender with the error message "Over quota".

In order not to exceed your allocated space, you should occasionally delete or archive your old messages (on your microcomputer or on a CD-ROM). Especially messages with large attachments should be removed from the server, as they take a lot of space.

A single message sent through the University mail cannot exceed 10 megabytes in size. Larger messages can be sent through the Hermes system. More info on our Web pages.

5.5. Additional Functionality

The e-mail system has normal additional functionality: e-mail can be forwarded, an automatic vacation message can be set etc. More information is available on our Web pages.

5.6. Mailing Lists

A mailing list can be created for organizations and other groups for internal communication. The list must have an administrator, who adds and removes recipient addresses as needed. Requests for new lists are sent to tunnukset@utu.fi. When the administrator changes, the previous administrator must notify the Computing Centre.

There are no general rules on the use of mailing lists. Some common protocols to go by are

People are not added to the list without their explicit permission as well as confirmation that they read their mail too

People who only seldom read their mail are not added to a high-traffic list, as the mail disk fills up with unread mail.

The list is not intended for commercial or any other use by anyone other than the organization who set up the list. If there's an event you wish to advertise, use news groups or Web pages (keeping in mind that the student organization home pages are not meant to be just market places). Bulk mailing advertisements to several lists is forbidden.

6. Data Storage Services

The computers connected to the University network can use network drives to save their files. There are several advantages to using them:

- large files can be transferred from one place to another effortlessly, since the network drives can be accessed from any computer (in computer labs, for instance)
- network drives are regularly backed up on tape, which means that all files will automatically have at least some kind of a backup copy

The network drives have limited amount of space a lot less than most microcomputer hard drives. Really huge files (hundreds of megabytes in size) should be stored on the hard drive of a microcomputer, and backed up on a DVD-ROM, for instance.

6.1. Personal Home directory: "Oma verkkokansio"

Every user of has a personal home directory called "Oma verkkokansio" (roughly translates to "My network folder") which serves as his personal disk space. The contents of this directory are personal and can only be viewed by the owner. The directory has 500 megabytes of space per user. If you need more space, you can ask for it from **levypalvelut@utu.fi**

To access your home directory, you will have to log on the UTU domain with the miccomputer network password.

When logged on to a Windows 2000/XP workstation, your "Oma verkkokansio" is located either on the desktop as **My Documents** (in most computer labs) or under My Network Places at **Oma Verkkokansio**.

6.2. Personal www-folder

Every user also has a personal WWW directory. This directory has 100 MB of space, and it is reserved for the personal home page of the user.

To access your WWW directory on a Windows 2000/XP click on **My Network Places** and select "**Oma WWW-kansio**" (roughly translates to "My WWW folder")

6.3. Other network drives

In addition to the aforementioned there are also other network drive resources (Web pages for the departments or student organizations, program installation disks, departmental disk spaces). More information on these is available on the Web.

The unix.utu.fi mainframe also has its own network drives.

7. Other services

7.1. Wentti

Wentti is a service used to view test results online. The results are indexed with student numbers. The service is in Finnish, but if you know the name of the course you are taking, you should be able to use it with minimal knowledge of the language. Wentti can be accessed from anywhere with username and e-mail password. It is at

<http://www.utu.fi/opiskelu/wentti/>

7.2. Calendar

There is a calendar server, which can be used to store personal or shared calendars. You can log on to it from anywhere with your username and e-mail password. It is found at the address <https://calendar.utu.fi/>

7.3. IRC service

The University has an Internet Relay Chat (IRC) server at the address <irc.utu.fi>

7.4. Unix

There is an unix server available at unix.utu.fi. User account for the server can be activated on request. Most users don't require it.

7.5. Library services

The University Library provides several scientific journals online. You can access these journals without a password from anywhere in the University, or with a username and e-mail password from anywhere in the world. The Library services can be found at <http://kirjasto.utu.fi/english.html>

7.6. eWert Online Newsletter

University Communications & PR Department publishes a monthly online newsletter called eWert. It is mostly in Finnish. It requires a username and an e-mail password. eWert is at <https://intra.utu.fi/>

7.7. Et cetera

A comprehensive list of other services does not fit into this manual. More information is available on the Web pages of the Computing Centre.

8. Connecting from Outside the University

8.1. Modems

The university has a modem pool, which is accessible to all users. Using the modem pool is free. The telephone company will naturally charge a normal charge for calling. The modem pool requires the e-mail password for logging on. The number is 02 334 9000.

8.2. The Student Village Network

In the renovated apartments of the Student Village it's possible to connect a home computer

directly to the university network. Opening a student village network connection requires filling in an application and returning it to the Computing Centre in person. The registration fee is 60 € for students of the University, the monthly cost is included in the rent. Matters concerning the Student Village Network are handled by the Help Desk of the Computing Centre.

Connection costs, troubleshooting information and other important data can be found at the Student Village Network home page, <http://www.yok.utu.fi/>. There is also a separate manual (both in Finnish and English) available at the Computing Centre Help Desk. Help with problems concerning the Student Village network is available from kylapulma@utu.fi.

8.3. The College ADSL

The College ADSL is a direct home connection to the University network that uses telephone cables. This type of connection is being phased out, so it's probably better that an ADSL connection is subscribed directly from a phone company than through the university.

8.4. Remote Connections to University Services

It's possible to access some microcomputer network services from outside the University network, such as the personal network folder or the Web folder. This is mostly done by using the Citrix Presentation Server system of the University. By installing a Citrix Presentation Server Client program on a microcomputer anywhere in the world you can open a remote connection to the University network, and use your own network folders or programs on the remote access server (e.g. Microsoft Office). In addition to a Metaframe client program this requires a username and a microcomputer network password.

8.5. Connections with Mobile Devices

It is possible to access University network services remotely with mobile devices (ie. network phones and PDAs). In theory the services are limited only by the capabilities of the device. The most requested service is e-mail, but checking test scores, using the Electronic Reading Room and even accessing University network drives (through a Presentation Server connection) are also possible.

The Computing Centre tries to support mobile devices if it has resources. The list of supported devices is far from all-encompassing, and some devices simply lack the necessary features to utilize the University services (e.g. the device may not have sufficient encryption capabilities for e-mail use). Devices that are the property of students and staff instead of the University are technically outside the scope of support, but the instructions we provide should still be useful.

If you are considering a mobile device you should probably have a look at the information on our Web pages. We have detailed instructions for some devices, general information that should help with others, and information on devices we have been unable to get to function properly with the University services.

9. User Account Regulations: Students

This is a contract specifying the conditions for use of IT services provided by the University of Turku. The user agrees to abide by the terms of the contract, instructions given by the Computing Centre, good manners and the law. For using the modem lines of the university the user agrees to pay the current service prices charged by the Computing Centre (at the moment free of charge).

1 The Rights and Obligations of the User

1.1 User Account and Password

The Computing Centre issues the user accounts and passwords. Both are for personal use only. The user is responsible for the use of his/her user accounts, as well as the secrecy and regular changing of the passwords. The user accounts are not to be rented out, sold, lent or otherwise passed on to be used by another person or juristic person.

1.2 Appropriate Use

The user account is to be used primarily to support teaching, studies, research and university work. The publication or distribution of commercial material, illegal material or material contrary to good manners, or the unnecessary taxing of system resources is not permitted. Sending chain letters, or bulk e-mail targeted to an unspecified list of recipients is explicitly forbidden. The user account may not be used to seek out data security breaches, or for any other kind of system intrusion. The user must immediately notify the administration of any data security breaches he/she has noticed. Trying to obtain information on a text, image, data transfer or other similar electronic message the user has no permission to is forbidden and can lead to charges for a communications crime. The user is not allowed to give or sell network services of his own server to a third party without a specific agreement with the Computing Centre. The user is required to abide by all instructions and regulations issued by the Centre concerning the use of the user account and the network services provided by the Computing Centre. Information on these instructions is available at the Computing Centre, or at the WWW pages at <http://www.cc.utu.fi/en/>.

The user of the service is liable for damages caused by action contrary to the terms of this contract, or otherwise intentionally or accidentally caused by the user.

2 The Rights and Obligations of the Services Provider

The Computing Centre is responsible for the functionality of the service. The service includes user accounts on the servers and the permission to use the services of the university network. The Computing Centre is not responsible for economical losses or other damages due to technical problems, network load or service breaks caused by administrative action. The users will be notified in advance of service breaks of substantial duration required by maintenance. Any malfunctions will be handled mainly during office hours. The service does not include correcting problems caused by hardware or software of the user.

As a temporary measure, the Computing Centre reserves the right to without prior notice

limit the use of services causing substantial load on the network or the university computer system, or which can harm the Computing Centre as a service provider due to action that is contrary to law, good manners, the terms of this contract or instructions of the Computing Centre. As a protective measure the Computing Centre has the right to disconnect the trouble causing workstation, server or other device and to close a user account if a user has not changed the password for a long time, or if the password is otherwise found to be easy to discover. In order to look into suspected misuse, the Computing Centre can check material saved under the user account and processes owned by the account.

3 Changing the Terms of the Contract and the Prices of Services

The Computing Centre has the right to change the terms of this contract and the prices charged for services. The changes are effective immediately, except for changes in service costs, which are effective starting at the beginning of the next month at the earliest. Information on changes is displayed at <http://www.cc.utu.fi/en/>, and when needed, it can also be sent personally via e-mail.

4 Termination of the Contract

This contract is valid as long as the user is a student or an employee of the University of Turku. The contract is automatically terminated when the studying or employment comes to an end, and also if the user doesn't fulfil his contractual obligations or otherwise uses the computer services of the university contrary to the terms of this contract or to the instructions or regulations of the Computing Centre. At the termination of the contract the user is required to pay for services received according to the current service price chart. Both parties have the right to terminate the contract by issuing a written statement to the other party. The termination is valid as of the day mentioned on the statement.

5 Transferring the Contract

The user does not have the right to transfer the contract or rights inherent in it to a third party.

6 Other

Current user account terms and instructions and regulations relating to them can be found on the WWW page <http://www.cc.utu.fi/en/>. The page is also used to inform users of any changes to the terms and regulations of use, as well as for instructions how to use the computer.

