

STUDENT'S MOBILE SECURITY GUIDELINES

Mobile devices (smart phones and tablets) can easily get lost or stolen. Therefore, they entail the risk of unauthorised access to the user's or university's data. Unauthorised users can also pose as the device owner and send e-mail in his/her name. Hence, it is important to know the information security risks and act accordingly.

TAKING THE DEVICE INTO USE

- Write down the device's serial number, the phone's IMEI code and the subscription's identifier information. Keep this information in a place where you can easily find it when necessary.
- Mark your device, e.g. with a sticker and your initials, so that you can easily distinguish it from other similar devices in such situations as meetings or airport security checks.
- Always protect your device with a password or security code. Don't use birthdays or other easily figured numbers or words.
- Remember the device's security code. If you forget your security code, you can only regain access by restoring factory settings, which means that you will lose all data you have saved on the device.
- Find out whether your mobile device can be remotely erased if necessary and, if this is possible, how it is done.
- Find out which university services you can and are allowed to access with your mobile device.
- Consider installing an anti-virus software and firewall; there are many good alternatives available even free of charge.

USING THE DEVICE SAFELY

- Don't lend your mobile device to anyone.
- Lock your device when you are not using it. Many devices have an auto-lock feature that locks the device when it has been idle for a certain time.
- When you log into your device, make sure that no one sees your security code or password. Change the code if you have reason to suspect that someone has found it out.
- Some tablets and smart phones can be equipped with a so-called screen privacy filter that conceals visibility of the screen from the side.
- Don't open messages that come from unknown senders or seem suspicious for some other reason. They may contain malware that send messages in your name or cause other kinds of harm and extra costs.
- Don't install any software application you don't really need. Only download and install software from authorised distributors.
- Update all software regularly in order to ensure information security.
- Remember to take back-up copies of the material stored on your mobile device (or synchronise the device).
- If you synchronise e.g. the calendar and address book of your mobile device, you should use services approved by the university.
- Think carefully about what kind of information you can synchronise with an external network service.
- Consider whether it is necessary to publish your device's location information online.
- Disable wireless connections (Bluetooth and WLAN) when you don't need them.
- When travelling, avoid browsing the web and automatically synchronising your e-mail with the mobile device, because foreign data transfer costs are high.

IF YOU LOSE YOUR DEVICE

- If possible, erase the device contents remotely and then close the mobile phone's subscription. Note that remote erase is no longer possible once the subscription has been closed, so you might want to wait for the remote erase to be completed before closing the subscription.
- Notify IT support about losing the device.
- If the device was stolen, report it to the police.