Swedish Civil
Contingencies
Agency

Guidelines for smart phones, tablets and other mobile devices

10:46
77 %
Säkrare användning av surfplattor och smart...
www.msb.se/sv/Star
Läsare
Google
Säkrare användning av surfplattor och smarta telefoner

Summary

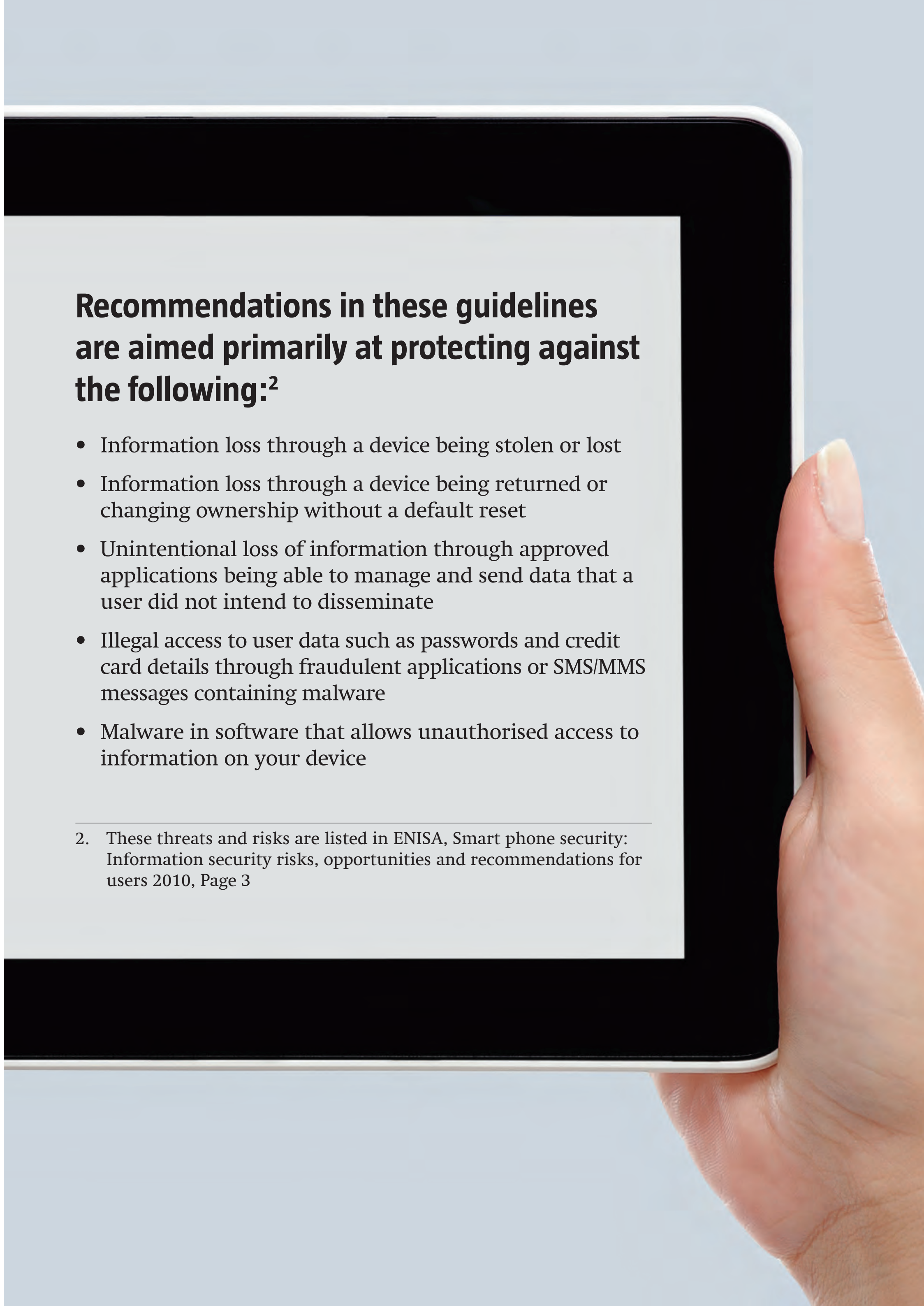
Smart phones, tablets and other similar mobile devices are being used increasingly both privately and in organisations. Another emerging trend is that users are given access to work-related information via their mobile devices. The increasing use of smart phones and tablets, in combination with the fact that both private and work-related spheres becoming ever more indistinguishable, means that operational information and information assets are being exposed in a new way through these mobile devices. This development is placing demands on organisations who want to use the technologies in a safe way.

These guidelines are intended to provide support for organisations that plan to allow smart phones, tablets or other mobile devices to connect to the organisation's internal resources and want to achieve this as securely as possible. The challenges are present to a large extent in education, management, regulatory frameworks and technical implementations for protection. These guidelines provide recommendations on what your organisation should regulate in the regulatory framework and procedures, what requirements should be imposed on the users and the technical protection that is recommended when mobile devices are allowed to connect to your organisation's internal resources

There are many different types of mobile devices. Smart phones and tablets are the more advanced devices under the generic term of mobile devices and these guidelines will use this in the first instance even though the recommendations in most cases are aimed at supporting the handling of smart phones and tablets in particular.

The basis for the selection of recommendations is a compilation of the most common action points in the internal rules that MSB has become privy to from a number of agencies and organisations. In addition, recommendations from the European Network and Information Security Agency (ENISA)[1] have also been considered.

[1] http://www.enisa.europa.eu/



Recommendations in these guidelines are aimed primarily at protecting against the following:[2]

- Information loss through a device being stolen or lost
- Information loss through a device being returned or changing ownership without a default reset
- Unintentional loss of information through approved applications being able to manage and send data that a user did not intend to disseminate
- Illegal access to user data such as passwords and credit card details through fraudulent applications or SMS/MMS messages containing malware
- Malware in software that allows unauthorised access to information on your device

[2] These threats and risks are listed in ENISA, Smart phone security: Information security risks, opportunities and recommendations for users 2010, Page 3

Background information

The use of mobile devices has increased greatly in recent years and this is predicted to continue to rise,[3] but uncertainties remain as to how these devices should be handled in an organisation and what protective measures should be taken.

The development and design of smart phones, tablets and other similar mobile devices has been mainly characterised by market demands for functionality, without focusing on and ensuring the security of the devices. Mobile devices like these can now often include personal information about the user, his/her contact networks and very often even user names and passwords to a variety of services. In assessing the need for protective measures, it should be taken into account that the more advanced mobile devices can be tracked, monitored and intercepted. It is quick and easy to install spyware and other malicious code, particularly if the devices fall into the wrong hands at an unguarded moment.

If information is stored on the mobile device, it is important that it is given adequate protection and the device is handled in such a manner that the potential for information exposure is minimised. Information on the mobile device needs to be protected to ensure it does not fall into the wrong hands, is manipulated or lost. Manipulation or loss of a mobile device that is used at work and that is able to connect to the organisation's internal network can be used as a springboard for further attacks on your organisation. For example, by reusing stored information for wireless networks, an attacker is given access to the organisation's internal resources. Depending on the aim of the attacker, this could lead to further serious loss of information, accessibility problems and loss of trust among partners and customers. The purpose of the protective measures is to provide a two stage effect; if the mobile devices get added protection to reduce the risk of an attack being successful, this also reduces the risk to the organisation's information assets and other resources being accessible to external attackers via mobile devices.

[3] See for example – Gartner Reveals Top predictions for IT Organizations and Users for 2012 and Beyond, *http://www.gartner.com/it/page.jsp?id=1862714*

Purpose

There are many different types of mobile device, all of which have different security requirements and risks. These guidelines use the term *mobile devices* throughout but the recommendations are in most cases designed to support the handling of the more advanced devices, primarily smart phones and tablets.

As supporting documentation for the choice of recommendations in these guidelines, MSB has used a compilation of the most common action points in the internal rules of a number of agencies and organisations, as well as recommendations from ENISA. The recommendations contained in these guidelines should be seen as "good practice", rather than "best practice" as there is a number of practical ways of solving the handling of mobile devices. As help when using these recommendations, they have been divided into three main groups based on the purpose they have and the target group they are aimed at:

- Recommendations for the design of regulatory frameworks and procedures
- Recommended requirements that should be imposed on users
- Recommendations for the design of technical protection

Working systematically with information security is a process that includes requirements set on the organisation, other players or legal regulatory frameworks affecting the design and selection of protective measures. Before recommendations are used, it is important to carefully analyse the protection needs the organisation has.[4]

[4] At *www.informationssäkerhet.se* there is support for how an organisation can implement a risk analysis and other measures linked to systematic information security management

An analysis of this type should be a part of a regular process and repeated as and when the requirements change. An organisation that currently does not allow connection of phones to internal resources does not need to address this in its rules and can obviously ignore the guideline recommendations in these sections. If circumstances were to change, the formulation of regulatory frameworks and procedures, requirements for users and technical protection should of course be reviewed.

In cases where the organisation owns the mobile device, it may be the organisation's regulatory framework pertaining to mobile devices that is easier to maintain. The organisation may require that the employee observes established rules regarding the handling of the mobile device but also installs software and introduces physical limitations on the device as a way of enhancing security. However, the user still has a major responsibility for the handling of the device. Mobile phones and tablets are perceived by many users as more of a "private" possession than, for example, a laptop, which is why the introduction of technical constraints to maintain the regulatory framework may meet some resistance among employees.

The following recommendations, Sections 2.2 – 2.4, are primarily intended to be used in cases where the organisation owns the mobile device. The main recommendation is not to allow privately owned devices to connect to an organisation's network. If this is nevertheless permitted, the overall recommendations are listed in Section 3 with respect to what you should consider and how to improve security.

The organisation owns the mobile device

One process and three tools for increased security

Building security in most cases requires a combination of measures, including both administrative rules and technical solutions. As mentioned above in Section 1.2, security management is also a process where the chosen measures need to be designed to ensure they match the ever-changing requirements and preferences of the organisation and environment. It is also important to ensure the organisation's security management in general, where the secure handling of mobile devices is a part of several interconnected elements.

On the website *www.informationssäkerhet.se* MSB, along with other agencies with special responsibility for information security in the community, has compiled a support package for systematic information security management in organisations. The primary aim is to help organisations to control and structure their information security management by introducing an information security management system (ISMS). Work to ensure the secure handing of mobile devices in the organisation should be an integral part of the organisation's overall information security management.

Information classification is a key activity in security management of mobile devices and is designed to assess the value of information and its sensitivity. The assessment is based both on individual operational needs and on external requirements. The intention is that each information asset (mobile device) is to be covered by the right protection.

In all areas of the security management, it is vital that those affected by the various measures have sufficient knowledge and understanding of what is required of them. Before a user signs for a mobile device, the user should be aware of, and should have accepted the user policies for the mobile device through a signature. This is to clarify that the user understands and is familiar with the adopted rules of the organisation.

Below is a summary of the recommendations; they have been grouped based on their purpose and the target group they have:

- *The recommendations for the design of the organisation's regulatory framework and procedures for the management of mobile devices* are made up of a summary of the issues that the organisation needs to take a position on. By way of example, it is recommended that the organisation determines the services that are to be accessible from the mobile device. The choice of the services that are actually made available should be based on a risk analysis.
- *When it comes to the recommendations for the requirements that should be imposed on users,* the focus is on the requirements associated with "good practice" that are to be placed on the users. It is important to note that these recommended requirements do not constitute a complete set of user rules. Once the organisation has taken a position on how the more general regulatory framework and procedures are to be designed, the user rules will need to be supplemented to reflect these. To help users comply with the rules, it is important that these are grouped in one or a few documents, and that they are clear and easy to understand.
- *The recommendations for the design of technical protection* are specific and the consequences of departing from these recommendations should be carefully analysed. The introduction of technical protection may involve costs which of course should be balanced with the expected benefits/impact of the investment.

Each organisation designs its governing documents and rules in a way that suits its own operations. The aim of the classification above is primarily to clarify the purpose of each type of recommendation to ensure the organisation can incorporate the recommendations into its own documents in a simple way.

Recommendations for the design of the organisation's regulatory framework and procedures for the handling of mobile devices:

Determine the regulatory framework and procedures:

Connection, installation

- If the user is to sign for the mobile device in order to clarify the ownership relationship for the device.
- The way in which mobile devices can connect to the organisation's resources (wireless network, via cable, Bluetooth, etc.)
- The types and models of mobile devices that may be connected to the organisation's resources (e-mail, networks, etc.)
- The services (for example, e-mail synchronisation and access to internal network resources) that can be accessed from mobile devices.
- If a decision regarding the connection of mobile devices is to be documented. The user should acknowledge the decision which should include the services that are covered, who is covered as well as other responsibility relationships.
- How purchase and re-installation before use, such as reset to factory settings, should be managed. This is to reduce the risk of pre-installed malware.

Use and storage

- The type of information that may be allowed to discuss via mobile devices.
- How mobile devices are to be stored.
- The type of information that may be stored on the mobile device. The rules for the type of information that may be stored on mobile devices should be linked to the organisation's information

classification[5] system making it easy for the employees to understand. A mobile device should be considered as an uncertain media source to store information on.

- Whether, and if so how, external storage space in the mobile device in the form of items like memory cards are to be replaced and disposed of with a certain regularity.
- What applies to the use of mobile devices, for example, at meetings or conversations where sensitive information is being processed. At meetings of this type, these devices may perhaps not be allowed to be brought into the meeting room at all as they can act as listening devices without the user's knowledge.
- If internet surfing can be done directly from the mobile device, or if it has to go through the organisation's secure connection for improved control and protection of traffic.
- If the user is allowed to open SMS/MMS messages from unknown senders, or click on the links sent by unknown individuals/senders.
- If the user is to disable the automatic opening of messages.
- If and how the user is to install applications (apps). A user should only download applications that are needed to perform his/her work duties and that are from known and reputable libraries. A user should be aware of the functions and information the applications require access to.
- If the user needs to switch off the services that are not needed to perform his/her work duties, such as general location services, GPS positioning, WLAN, Bluetooth, GPS, data traffic, etc. This reduces the exposure of the mobile device and also saves the battery.

[5] MSB, together with the Swedish Standards Institute (SIS) has published a national model for information classification that aims to support government agencies and other organisations in their efforts to classify information in a uniform way. More details about this information classification are available at https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-fran-MSB/Stod--verktyg/.

- If the user must avoid posting images on the internet taken with the mobile device. Embedded meta data may reveal the time the photo was taken and its location.
- If the user is to regularly delete information that is no longer needed.

Security procedures

- How backups and synchronisation of devices may be made and the protective measures that apply to backups.
- If the user is responsible for updating the mobile device. Updates should be implemented as soon as the updates are available.
- Whether and if so how, logging applies to the use of mobile devices, and that follow-up can occur if this is the case.
- Who gets to decide on installing the various types of software in the device. to this decision, establish processes to manage the approval of security settings, applications, connections, etc. If the organisation has a "white list" of approved applications, users can install these themselves.
- How and at what interval the training of users needs be implemented. Training should include the handling of the mobile device as well as the risks associated with using them.
- Procedures for the secure handling and deletion of data on returned devices. A returned device may be reused within the organisation, passed on outside the organisation for continued use or be discarded. Devices that can no longer be used should be deleted of content or restored to factory settings before discarding.
- A process for the notification of loss, or if the mobile device has been manipulated.
- A process for the follow up of compliance with the organisation's internal regulatory framework and procedures. Follow up should be regular and structured through internal controls.

Recommendations for requirements that should be imposed on users

Determine in the user rules:

- The user is obliged to have physical control over the mobile device and does not leave it unattended, for example, in a public place, hotel or visible in a vehicle.
- Following loss of a device, how the user is to notify the organisation and if this should be done promptly.
- That the user must password protect the device to ensure it is locked when the screen saver is active. You are recommended to avoid the most obvious PIN or passwords such as 1111, 1234, and activation of the timing of inactivity before the screen saver is enabled.
- That the user cannot manipulate the mobile device's basic functionality, for example, getting a higher authority level in the device's internal file system.
- That the user is to avoid exposing the phone number and work-related e-mail addresses in situations that are not work-related. For example, it is inappropriate to add a phone number and e-mail address to the user's work on social media such as Facebook and Twitter if the work does not require it.
- That the user only uses the mobile device for Internet surfing in accordance with the organisation's regulatory framework.
- That the mobile device in the first instance is to be connected to known wireless networks that have protection in the form of encryption.
- That the user cannot change the SIM card in the device to use it for private purposes that do not comply with the organisation's regulatory framework.
- That the user is to immediately change the password of the services that the user is allowed to connect to if the mobile device has been stolen or lost.

Recommendations for the design of technical protection

- Allow only protected connection and storage for synchronisation of calendar, e-mail, contacts, etc., and implement a secure connection (VPN) to the organisation's internal resources. If extra protection is needed, consider implementing two-factor authentication.
- Implement encryption for the mobile device if this function is deemed necessary and if the technical conditions are in place for the mobile device. Information that may be stored and who may need protection in the form of encryption may consist of e-mails, attachments, documents, photos, login details, etc.
- Implement control functions for the relevant communications that go to and from the synchronisation points that the mobile device can connect to. Install protection to combat malware there (e-mail server, internal network resources, etc.).
- Implement centralised control over the organisation's mobile devices, where the update status, compliance with the regulatory framework, etc. can be monitored and measures can be taken, for example, when a device is lost.
- Implement processes to manage the loss of a device to ensure remote deletion of the data held on the device, and to lock the SIM card and IMEI number at the operator.
- Follow up the cost of the mobile subscriptions and be prepared to react to any anomalies.
- Implement solutions for the detection and protection against any malware in the mobile device.
- Implement processes to reset the infected mobile devices to a known safe setting, such as factory settings.
- Monitor the updates that are made available for the types of mobile devices and applications that the organisation uses.
- Implement a procedure to inform users when new updates are available. The time for security updates can vary greatly for mobile devices and are much less frequent than for computers.
- Where possible, limit the access rights of the mobile devices exclusively to authorised users.

A private individual owns the mobile device

A mobile device owned by an employee is entirely outside the organisation’s administrative jurisdiction, which means that the organisation has little ability to enforce its regulatory framework and technical restrictions. The mobile unit is likely to be used for a number of private purposes, and is therefore exposed in a way that the organisation is unable to influence other than by a separate agreement. The ability to follow up whether the employee is complying with the agreed rules is limited. The recommendation is therefore that, as a general rule, not to allow privately owned mobile devices to connect to the organisation’s internal resources and services such as e-mail, calendar, storage space for documents, etc.

If you nevertheless allow this, then you should take into account the recommendations for organisation-owned devices, but be aware of the difficulties of ensuring compliance with the rules. A decision allowing private connection to the organisation’s resources should be preceded by a thorough risk analysis. The employee should, in order to take advantage of the services offered by the organisation, even as a private individual commit to following the rules that the organisation stipulates. Sound knowledge of the user with respect to the risks associated with usage is important.

An organisation should also review whether there are technical solutions that can help in cases where privately owned mobile devices may be used, for example, as applications that are based on the principles for thin terminals. By way of example, there are solutions where no information is stored on the device, but the information is held centrally and users can “view” the information through the application.

Concluding reflections

Mobile devices are now an important tool and are a major source of information. Correctly used, smart phones, tablets and other mobile devices and all the new technology associated with them, can be important elements in our daily work without being a security risk for an organisation and its employees.

These guidelines for smart phones, tablets and other mobile devices should be seen as an aid in the systematic information security management in an organisation. More information and support on how an organisation can engage in information security management in its operations is available at *www.informationssäkerhet.se*.

Swedish Civil Contingencies Agency (MSB)
S-651 81 Karlstad   Phone +46 (0)771-240 240   www.msb.se/en
Order No. MSB531 - January 2013   ISBN 978-91-7383-319-6