SHIELD
Information Protection Newsletter
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
your energy partner®
OPPD
Omaha Public Power District

Protecting mobile devices

Mobile devices have become such a vital part of modern society. No longer just for making phone calls, modern mobile devices can send text, audio, and video messages, plus access Internet-based content through a myriad of applications. However, with greater convenience comes greater risk to personal data. Here are 12 top maxims for keeping cyber criminals from exploiting mobile devices.

Don't pass on passwords or passcodes. To protect yourself, be sure you lock your devices with a hard-to-guess password or passcode. As unpopular and sometime irritating as a locked mobile device can be, it does help keep thieves from getting sensitive data.

Install Anti-virus software. Now that there are a number AV apps for mobile devices consider installing one to protect against hackers and malicious software. Mobile devices are quite powerful and you'd be surprised what a hacker can do with a compromised tablet or cell phone.

There is no such thing as a secure mobile device. Regardless of operating system, mobile devices are subject to a variety of attacks, ranging from low-tech pick pockets to high tech wireless exploits.

There is no such thing as free. Free mobile apps, especially cool free mobile apps often mine your mobile device for personal information that is useful to marketers. When installing new apps, make sure you understand what permissions you're giving to the application. Be sure to read the app reviews so you can understand if the app is a threat to your privacy.

Install only the apps you need. Apps often come with subtle flaws that under the right circumstances can be exploited to expose your private data, so the more apps you install, the more vulnerable your device becomes.

Don't poison the well. Just in the same way you wouldn't intentionally poison your drinking water, don't download apps from third party sites or apps advertised in SMS messages. Use only reputable apps from trusted sources.

Avoid the disastrous follow-through. Think, think, think before you click. Avoid clicking on hyperlinks sent through SMS messages and other text messaging apps. In addition sending phishing email to get uses to click on malicious links, cyber criminals are sending malicious SMS phishing (SMishing) messages.

Simple to move means simple to lose. Mobile devices now have the power of desktops from just a few years ago. While hugely convenient and useful, mobile devices can be easily lost. Report the loss of a mobile device immediately to your supervisor. You need to ensure that sensitive information on your mobile device is encrypted and backed up in case it is damaged, lost, or stolen.

Keep your mobile device updated. As with many other computing devices, cyber criminals are constantly looking for programming flaws that will allow them access to the mobile device. Keeping your mobile's device's operating systems and applications updated at least once a month really helps

Don't give away the bank. Mobile devices are generally vulnerable to man-in-the-middle attacks where hackers place their devices between your mobile device and the Internet. Limit what you do on public WiFi. If you must access a sensitive site make sure you do not save your user credentials in your mobile browser or app. When using a browser, double-check the URL to make sure you are really going to the right place. Make use you log out of the site or app when finished rather than just closing the browser or app.

Don't get conned. Legitimate businesses will not text or email you, asking for your logon credentials. Always contact the business directly, using a phone number from some source other than a sketchy email or text. When in doubt don't respond to suspicious email, texts, or phone calls.

Pull the fangs of Bluetooth attacks. Turn on Bluetooth only when you need it. Ensure that this short-range wireless protocol is configured so your mobile devices are not discoverable. This prevents information theft and device compromise in public places like restaurants, hotels, and airports.

For further assistance for your mobile devices, contact IT Service Desk.

Physical Security

Always have your work badge showing. In addition, be sure to question anyone else who does not have their badge visible.

your energy partner
OPPD
Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

IT Service Desk

© The SANS Institute 2014

At home or at work

Protect sensitive data

You can apply the saying “Familiarity breeds contempt,” to data security. Here are steps to secure sensitive data and avoid becoming numb to sensitive data exposure.

Always understand the nature of the sensitive information you handle and how it can be misused to harm OPPD, its customers and employees. If you are unsure how sensitive data should be stored talk to your supervisor.

Use only OPPD computer resources cleared to handle sensitive data. Don’t copy or store sensitive data on unauthorized systems or accounts, such as personal mobile devices, personal email accounts like Gmail or Yahoo, and cloud-based file sharing services.

If you must transfer sensitive data, use secure, authorized methods that support encryption. Do not send sensitive information by insecure means such as plain text email.

You must have prior approval to store sensitive information on removable media or portable storage devices. Sensitive information transported on these devices should be encrypted using an approved encryption method.

Be careful when responding to emails or phone calls. Always ensure the requestor is cleared to access sensitive data.

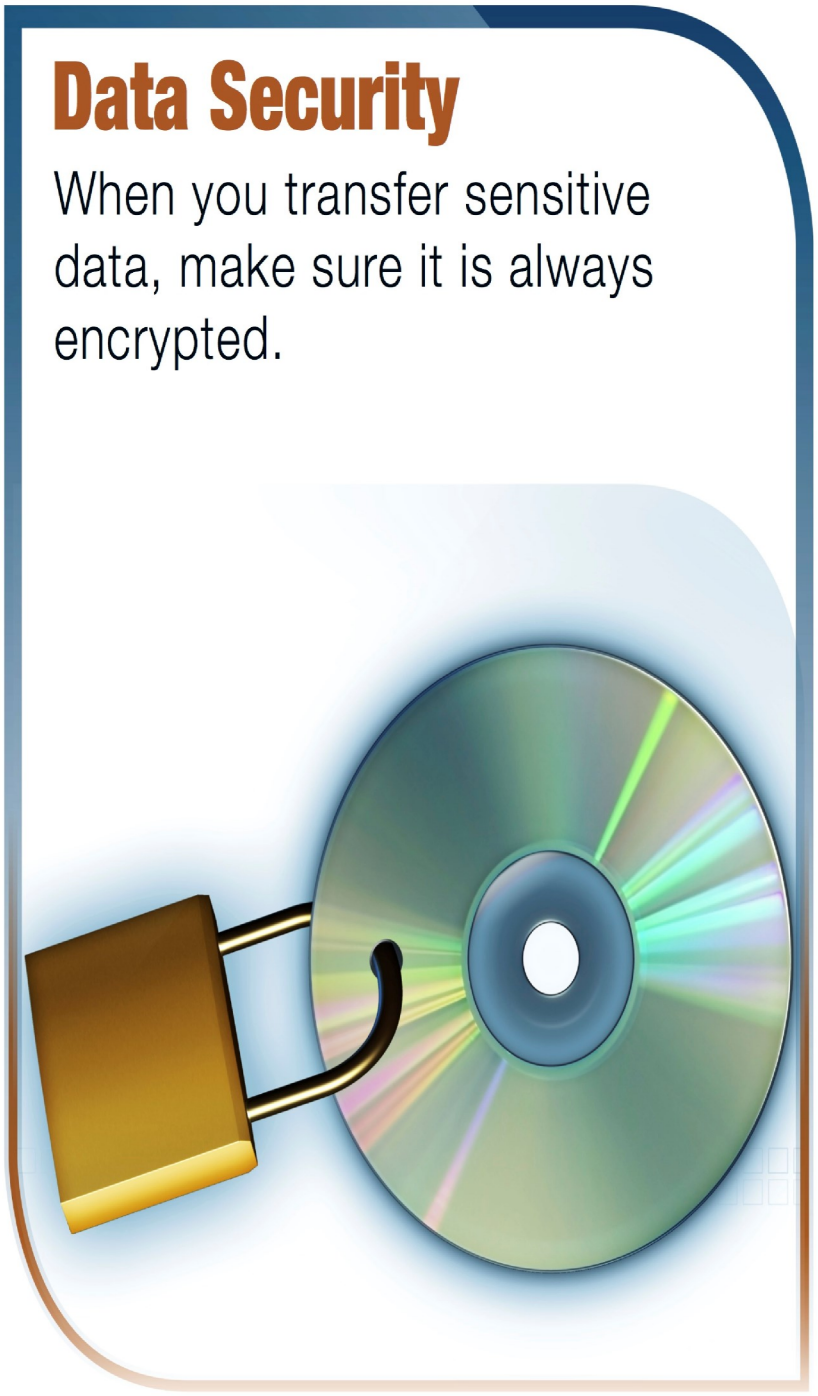
Ensure sensitive information is backed up and properly protected.

Don’t leave sensitive data unattended on desktops or at printers and fax machines.

Ensure you process sensitive information using authorized software.

Destroy information that is no longer needed or inappropriate to store, using approved destruction methods.

You are on data security front line. If you believe sensitive data has been compromised, contact the IT Service Desk immediately.



Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

IT Service Desk

© The SANS Institute 2014

North American Electric Reliability Corporation (NERC)

Quarterly Update

NERC CIP-006-6 R1.3

Two-Factor Authentication

Requirement 1.3

Where technically feasible, utilize two or more different physical access controls to collectively allow unescorted physical access Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

As NERC was developing version 5 of the Cyber Infrastructure Protection (CIP) standards, a directive from the Federal Electric Reliability Corporation (FERC) discussed utilizing two or more different and complementary physical access controls to provide defense in depth needed to be addressed. CIP-006-6 R1.3 addresses the FERC directive and changes the culture for many power generating entities. OPPD has responded to the challenge and beginning October 1st, will be implementing two factor authentication at specific NERC CIP facilities and locations. OPPD personnel who have unescorted physical access into NERC CIP areas will now require to access elements in order to enter NERC CIP areas:

NERC CIP Access Badge

5 digit access PIN

OPPD's Corporate Security and Support Operations department is heading up this project and has installed badge readers with PIN pads to meet this requirement. Over the last month, OPPD personnel with unescorted physical access into NERC CIP areas have been receiving notifications to attain their NERC CIP access PINs. OPPD sponsors are responsible for communicating the two factor authentication access methods to their respected contractors. Please keep in mind of the following information:

Contractors with NERC Access Authorization:

OPPD sponsors of NERC Authorized contractors need to inform the contractors of the requirements of two forms of authenticity. Contractors can obtain their PIN when obtaining their NERC access card at Central Station or ECC security.

To alleviate future issues, if you have are authorized for unescorted physical access into NERC CIP areas or are an OPPD sponsor who has contractors that have unescorted physical access, please ensure to attain your NERC CIP Access PIN as soon as possible.

For more information pertaining to NERC CIP Version 5, please contact Reliability Compliance Specialist, Mike Nickels, manickels@oppd.com; (402) 552-5036.

References

North American Electric Reliability Corporation. "CIP-006-6 Cyber Security." *Physical Security of BES Cyber Systems*. NERC, 28 October 2014.