your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Securing your Mobile Device, WiFi, & Data

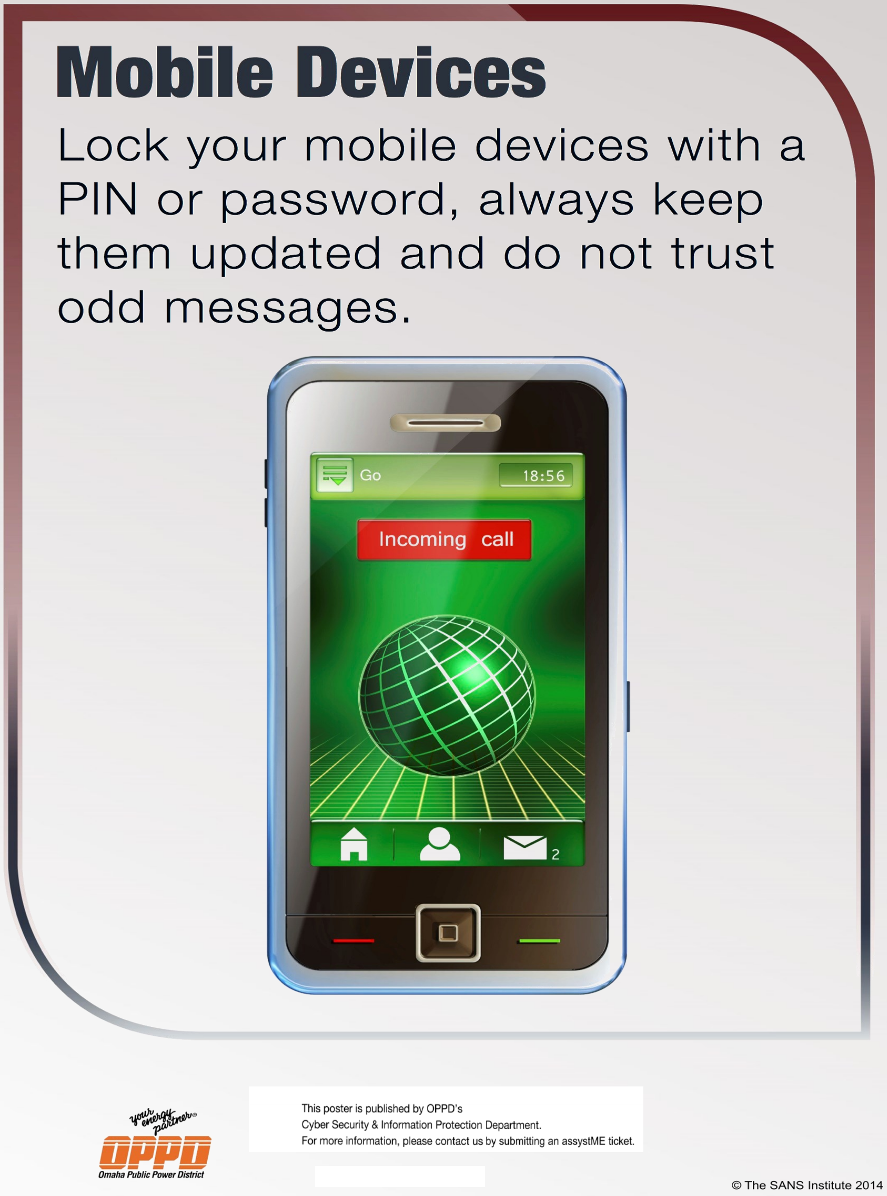
Securely Using Mobile Apps

Mobile devices, such as tablets, smartphones, and watches have become one of the primary technologies we use in both our personal and professional lives. What makes mobile devices so versatile are the millions of apps we can choose from. These apps enable us to be more productive, instantly communicate and share with others, train and educate, or just have more fun. However, with the power of all these mobile apps comes risks. Here are some steps you can take to securely use and make the most of your mobile apps.

Obtaining Mobile Apps

The first step is making sure you *always download mobile apps from a safe, trusted source.* Cyber criminals have mastered their skills at creating and distributing infected mobile apps that appear to be legitimate. If you install one of these infected apps, criminals can take complete control of your mobile device. By downloading apps from only well-known, trusted sources, you reduce the chance of installing an infected app. What you may not realize is the brand of mobile device you use determines your options for downloading apps.

For apple devices, only download mobile apps from the Apple App Store. The advantage to this is Apple does a security check of all mobile apps before they are made available. While Apple cannot catch all the infected mobile apps, this managed environment helps to dramatically reduce the risk of installing an infected app. In addition, if Apple does find an app in its store that it believes is infected, it will quickly remove it. Windows Phone uses a similar approach to managing applications. Android mobile devices are different. Android gives you more flexibility by being able to download an app from anywhere on the internet. However, with this flexibility comes more responsibility. You have to be more careful about which



Mobile Devices

Lock your mobile devices with a PIN or password, always keep them updated and do not trust odd messages.

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 by submitting an assystME ticket.

© The SANS Institute 2014

(Continued on page 2)

(Continued from page 1)

mobile apps you download and install, as not all of them are reviewed. Google does maintain a managed mobile app store called Google Play. The mobile apps from Google Play have passed some basic security checks. As such, we recommend you download your mobile apps for Android devices only from Google Play. Avoid downloading Android mobile apps from other websites, as anyone--including cyber criminals--can easily create and distribute malicious mobile apps and trick you into infecting your mobile device. As an additional protection, install anti-virus on your mobile device when possible. Regardless of which device you are using, an additional step you can take is to avoid apps that are brand new, that few people have downloaded, or that have very few positive comments. The longer an app has been available, the more positive comments it has, the more likely that app can be trusted. In addition, install only the apps you *need* and *use*. Ask yourself: "Do I really need this app?" Not only does each app potentially bring new vulnerabilities, but also new privacy issues. ***If you stop using an app, remove it from your mobile device. You can always add it back later, if you really need it.*** Finally, never jailbreak or root your mobile device. This is the process of hacking into it, and installing unapproved apps or changing existing, built-in functionality. This not only bypasses or eliminates many of the security controls built into your mobile device, but often also voids warranties and support contracts.

Permissions

Once you have installed a mobile app from a trusted source, make sure it is safely configured and protecting your privacy. Always think before allowing a mobile app access: Do you want to grant the app the permission it asks for, and does the app really need it? For example, some apps use geo-location services. If you allow an app to always know your location, you may be allowing the creator of that app to track your movements, even allowing the app author to sell that information to others. If you do not wish to grant the permissions, den the permission request or shop around for another app that meets your needs. Remember, you have lots of choices out there.

Updating Apps

Mobile apps, just like your computer and mobile device operating system, must be updated to stay current. Criminals are constantly searching for and finding weaknesses in apps. They then develop attacks to exploit these weaknesses. The developers that created your app also create and release updates to fix these weaknesses and protect your devices. The more often you check for and install updates, the better. Most devices allow you to configure your system to update mobile apps automatically, which is recommended, or at least every two weeks. Finally, verify any new permissions they may require.

JOSHUA WRIGHT Instructor, SANS Institute

Where are you hooking up?
HACKERS LURK ON OPEN NETWORKS
I'M A BAD APP
YOU CAN TRUST ME!
pick me!
helloooo!
BEWARE: FREE APPS CAN CARRY INFECTION
hey there...
I'm wiped out!
YOU ARE IN MY POWER AND WILL DO AS I SAY. . .
i'm out of here
Symantec.

KEEP YOUR PESKY HANDS OFF MY MOBILE DATA!

TURNING IT ON

Set up a strong password for your device (think combination of capitals, numbers and special characters) and ensure it has an automatic wipe function to kick in as a result of password failure – **this is the first and simplest step to protect your sensitive company data**

CONTROL YOUR CONNECTIVITY

Turn off your Bluetooth and deactivate the automatic connection to Wi-Fi, this setting can automatically be connecting to any/every public network wherever you go - **avoid hooking up to any old network or you risk having to explain to your boss where you have been**

BE CAREFUL WHAT YOU DO IN PUBLIC

If you want to participate in open networking and hotspots, then ensure you stay safe – always check the network is the genuine version and secure - NEVER access sensitive company information or online banking on a public network

YOU CAN'T TELL IF AN APP IS INFECTED JUST BY LOOKING

Only download from trusted or approved sources - bad apps can carry malware, viruses, spyware and worms - **never allow apps to 'remember' your passwords**

KEEP IT HEALTHY

Only download company-approved operating system updates to keep your mobile device in full health and on top of the latest security threats – your IT department is there to make sure all of your security holes are patched

IT ONLY TAKES A FEW SECONDS...

to have your mobile device stolen – are you prepared to tell your boss you have just lost the latest sensitive company information? (If you phone is stolen report it to the IT department immediately)

DO IT BY REMOTE CONTROL

If all else fails you can do-it-yourself – take back control by installing a remote-wipe app to ensure your sensitive work data doesn't fall into the wrong hands

DON'T GET CAUGHT IN COMPROMISING SITUATIONS:

DOWNLOADING APPS
PUBLIC WI-FI/HOTSPOTS
SOCIAL NETWORKS PHISHING
EMAIL PHISHING
SMS PHISHING

TAKE CARE:

ONLINE BANKING
OPEN NETWORKS

PROTECT:

WORK AND PERSONAL DATA

JAILBREAK PHONES ARE MORE AT RISK

Jailbreaking is the process of removing the limitations on some mobile devices to allow the use of unauthorized software and apps **but at the same time this opens your device, and the data it contains, to the threat of hackers and infected apps**

Understanding Encryption

Encryption is a mechanism that protects your valuable information, such as your documents, pictures, or online transactions, from unwanted people accessing or changing it. This works by using a mathematical formula called a cipher and a key to convert readable data (plain text) into a form that others cannot understand (cipher text). The cipher is the general recipe for encryption, and your key makes your encrypted data unique. Only people with your unique key and the same cipher can unscramble it. Keys are usually a long sequence of numbers protected by common authentication mechanisms, such as passwords, tokens, or biometrics (like your fingerprint).

REMEMBER:

- Encryption is only as strong as your keys; if your key is compromised, so is your data. Protect them well.
- Don't lose access to your keys. If you lose the encryption keys or can't access them (forgot password), you most likely cannot recover your data.
- Your encryption is only as strong as the security of your devices. If your device is infected, the bad guys can compromise your encryption.
- Maintain the security of your device against viruses, worms, etc.
- Back up confidential data securely to be able to recover it, if needed
- Consult an IT professional if you need help. Incorrect installation, configuration or usage of encryption can make your data permanently inaccessible.

FRED KERBY, Sr. Instructor with SANS Institute.

Wi-Fi Security

Always use encryption when connected over public Wi-Fi networks.

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us by submitting an assystME ticket.

© The SANS Institute 2014

Data Security

When you transfer sensitive data, make sure it is always encrypted.

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us by submitting an assystME ticket.

© The SANS Institute 2014

Encrypting Information in Transit

Information is also vulnerable when it's in transit. If the data is not encrypted, it can be monitored and captured online. This is why you want to ensure that any sensitive online communications, such as online banking, sending e-mails, or perhaps even accessing your Facebook account, are encrypted. The most common type of online encryption is **HTTPS**, or connecting to secured websites. This means the traffic between your browser and the website is encrypted. Look for **https://** in the URL or the *lock icon* in your browser.

Many sites support this by default (such as Google Apps), and websites like Facebook and Twitter give you the option in your account settings to force HTTPS. In addition, when you connect to a public Wi-Fi network, use an encrypted network whenever possible. WPA2 is currently one of the strongest encryption mechanisms and the type you should choose. Finally, whenever sending or receiving e-mail, make sure your email client is set up to use encrypted channels. One of the most commonly used is SSL (Secure Socket Layer); many e-mail clients use SSL by default.

Francesca Bosco is a researcher and a project officer, managing projects related to cybercrime, cybersecurity, and the misuse of technology. She is working at the United Nations Interregional Crime and Justice Research Institute and she co-founded the Tech and Law Center.

North American Electric Reliability Corporation Quarterly Update

CIP-007-6 Requirement 5 – System Access Control

As hackers have developed more tools to crack weak and ineffective passwords to gain access to critical systems, system passwords have become a major risk factor. In fact, the element of system security and the passwords used to access critical systems is nearly futile in remaining secure, compliant and overall reliable. With that being said, NERC does not minimize the risk of a hacker gaining access to the bulk electric system (BES).

Organizations that implement a password program, encompassing strong passwords or pass-phrases which are modified at a minimum of an annual basis, pose a stronger position to ensuring their systems remain secure against unauthorized access attempts. **CIP-007 Requirement 5** specifically address security elements all registered entities must implement to strengthen their security posture.

CIP-007-5.1 – For HIGH BES Cyber Systems, entities must have a method to enforce authentication of interactive user access. This requirement ensures the entity has electronic security measures in place to enforce authentication of access.

CIP-007-5.2 – For HIGH BES Cyber Systems & MEDIUM BES Cyber Systems, entities must identify and inventory all known default or generic accounts. Identification can be performed by system, groups of systems, by location, or by system type. This requirement ensures the entity has properly identified and inventoried systems which possess default or generic accounts.

CIP-007-5.3 – For HIGH BES Cyber Systems, entities are required to identify individuals who have access to shared accounts. Similar to R5.2, this requirement ensures entities identify and document all shared accounts on critical systems.

CIP-007-5.4 - For HIGH BES Cyber Systems & MEDIUM BES Cyber Systems, entities must change the known default passwords, per the system capability. This requirement has been established to remove passwords generated from system manufacturers, vendor passwords, or any password that can be researched from a manufacturer's website.

CIP-007-5.5 - For HIGH BES Cyber Systems & MEDIUM BES Cyber Systems, entities must implement, either technically or procedurally, password length and password complexity standards. This requirement sets the security standards for passwords. In the eyes of a hacker, the longer and the more complex the password is, the harder it is to gain access.

CIP-007-5.6 - For HIGH BES Cyber Systems, entities, either technically or procedurally, must enforce password changes or set an obligation to change the passwords at least annually. This requirement ensures the passwords in place will be modified on an annual basis.

CIP-007-5.7 - For HIGH BES Cyber Systems, where technically feasible, entities must limit the number of unsuccessful authentication attempts or generate alerting after reaching a set threshold of unsuccessful authentication attempts. This requirement focuses on monitoring and alerting of interactive access to critical systems. Limiting the login attempts until the user is locked out and performing alerting is another "defense in depth" approach to security.

Resources:

(North American Electric Reliability Corporation, 2016)

For more information pertaining to CIP-007 – System Access Control,

please contact OPPD's Reliability Compliance Specialist,

Mike Nickels – (402) 552-5036; manickels@oppd.com