The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- Precautions You Can Take Now
- What to Do If Your Device is Lost or Stolen

Losing Your Mobile Device

GUEST EDITOR

Heather Mahalik is the guest editor for this issue. She is a certified SANS instructor and the Mobile Device Forensics Technical Lead for Basis Technology, working out of Washington, DC. Heather is active on Twitter @heathermahalik.

OVERVIEW

Mobile devices are used for communication and for obtaining and sharing information. As a result, they often contain sensitive information, including email, text messages, voicemail, calendar events, location tracking, photos and videos. If your mobile device is lost or stolen, anyone who has physical access to your device can potentially access all this information and expose you, your contacts and your organization to serious risk. In this newsletter, we discuss the steps you can take to protect the information on your device in case it is lost or stolen.

Note: Most of this advice applies to your personal devices. If your mobile device was issued or authorized by your organization and contains organizational data, then be sure to follow your organization's policies for securing mobile devices and for reporting loss or theft.

PRECAUTIONS YOU CAN TAKE NOW

One of the most effective ways you can protect your information is to secure your device while you still have it. A great place to start is enabling some type of access protection, such as a PIN, password or pattern lock. This helps ensure that only authorized users can use and access the information on your device.

- **PIN**: A PIN (Personal Identification Number) is a number you have to enter to gain access to your mobile device.
- **Password**: A password on mobile devices works the same way as a password on your computer or online account. This is an option you can enable on most smartphones. A strong password affords greater security than a PIN.
- **Pattern Lock**: A pattern lock is a unique pattern that you draw on the screen of the device.

Strongly consider enabling the option to wipe your device after a certain number of failed access attempts, which can protect your device if it falls into the wrong hands. However, if you do enable this feature, be cautious of curious children. Regardless of the authentication

Losing Your Mobile Device

mechanism you use, make sure that you do not share your PIN, password or pattern lock with anyone else and that it is hard for people to guess.

- **Remote Tracking & Wiping**: Most mobile devices support software that can remotely locate and/or remotely erase your information from a missing device. You may have to install or configure special software while you still possess the device. iPhones and iPads come with this feature, called "Find My iPhone," and it is enabled using an Apple ID. BlackBerry devices must be tied to a BES server or similar application in order to remotely wipe your device. Android devices must have special software installed for remotely locating and wiping your device.
- **Encryption**: If someone has physical access to your mobile device, they can use advanced technologies and attempt to bypass your password or PIN and access the data stored on it. Encryption protects your data against these more advanced types of attacks. Some mobile devices come with encryption built in, while others require you to enable the functionality or install encryption software. iPhones and iPads provide built-in hardware encryption that is automatically enabled. Without your password, your data is protected. The Android has built-in encryption that can be activated in the Security menu.
- **Backups**: Backups help ensure you can recover your information quickly from a lost or stolen device. Backups should be performed regularly, and can be done using the following methods:
    - Backup directly to your computer.

By taking some simple steps now, you can protect yourself if you lose any of your mobile devices.

    - iCloud is provided as a free service to all iPhone, iPad and iPod users. The user can select to back up their contacts, email, calendar, pictures, music and other files to an iCloud account.
    - Google Cloud is a free backup service for Android devices. The features of the Google Cloud are similar to the iCloud.

Losing Your Mobile Device

WHAT TO DO IF YOUR DEVICE IS LOST OR STOLEN

Follow these steps to protect your personal information if your device is lost or stolen:

- If the missing device was issued to you by your employer or contains work-related data, then report the loss immediately to your organization's help desk or security team and follow their instructions.
- If you installed tracking software on your mobile device, you will most likely have the option to wipe your data. Wiping the device will erase all of your personal information from the device and eliminate the risk of your data being accessed. If your device was stolen, you may want to contact law enforcement before wiping the device and notify them that you have enabled location tracking on the device. If stolen, you should not attempt to recover your device yourself.
- Contact your Network Service or Phone Provider to alert them that your mobile device has been lost or stolen. They may be able to put a lock on your phone number to ensure no one can use your device to make any phone calls until you get it replaced.
- Once you have purchased a replacement, you can use your backups to recover your information.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

20 Android Security Apps:
http://preview.tinyurl.com/27qbb6w

10 iOS Security Apps
http://preview.tinyurl.com/bumb8vv

Google Cloud:
http://preview.tinyurl.com/cy49ntb

iCloud:
https://www.icloud.com/#find

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

BECOME A SECURITY PROFESSIONAL

Become a certified security professional from the largest and most trusted security training organization in the world at SANS 2013. Over 40 security classes taught by the world's leading experts. March 08-15, 2013 in Orlando, FL. http://www.sans.org/event/sans-2013/

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner