Think HR
Human Powered

# CYBERSECURITY PART 2:
# YOUR MOBILE DEVICE IS A BIG SECURITY RISK

Think HR
Human Powered

# CYBERSECURITY PART 2: YOUR MOBILE DEVICE IS A BIG SECURITY RISK

Corporate networks in companies of all sizes are under siege by a growing number of increasingly sophisticated attacks from cyber criminals across the world. These attacks can happen at any time, both to your business or to you personally on your own private networks. There are steps you can take to reduce the risks as the first line of defense against data breaches, malware infiltration and various other security risks.

This is Part 2 in the series of prevention steps you can take to help make your information networks more secure.

**Things have changed over the past few years...cyber criminals are now focusing increasingly on you and your fellow users as the weak link in the security chain.**

## You...

*are the primary line of defense in preventing really bad stuff from happening in your company and to yourself.*

**There is nearly a one in four chance...**
*that you will mistakenly click on a phishing email.*

**One click on a phishing email...**
*could cost your firm $377 per employee.*[1]

**A single Trojan horse exploit...**
*caused the State of California to shut down a business a few days after the attack occurred.*[1]

**One stolen laptop...**
*from the car of an HR professional who worked for Godiva Chocolatier revealed the names, addresses, Social Security numbers and drivers' license numbers of other employees.*[1]

Edition: 4.2116

# Your Mobile Device Is a Big Security Risk

## Your Smartphone Is Full of Data

The growing use of mobile devices creates an enormous security risk given that 66% of employees use their own devices for work-related purposes.[2] Your mobile devices contain a significant proportion of your company's data, including email, files, contacts, calendar appointments, customer information and other potentially sensitive and confidential data. As shown in *Figure 1,* users' smartphones and tablets contain 6% of the typical company's data; when laptops are added to the mix, however, more than 20% of corporate information is housed on a mobile device.

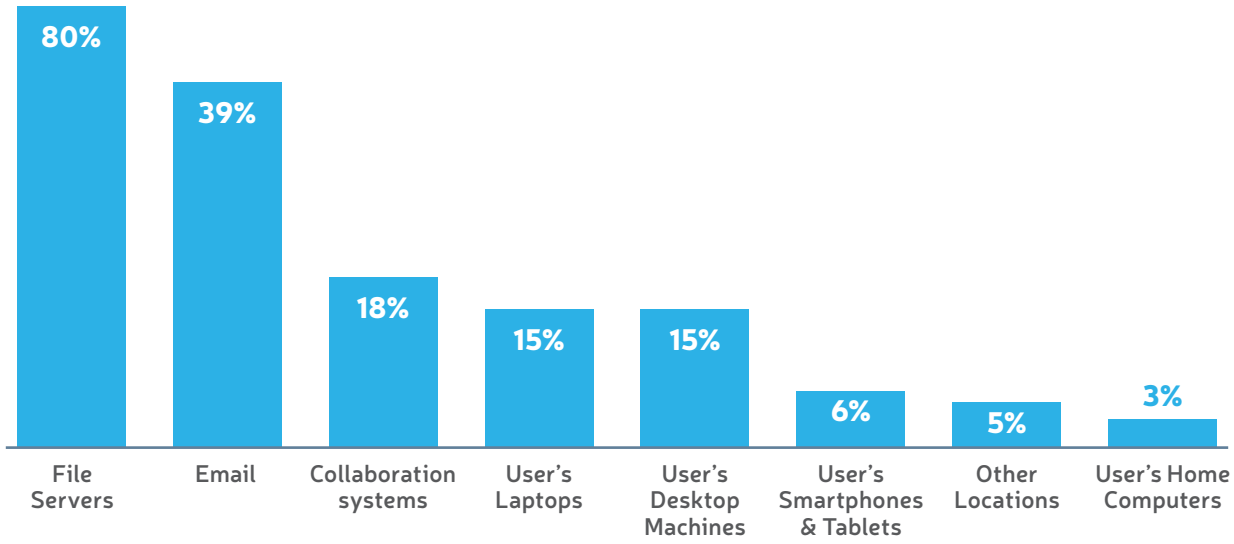


Figure 1: Distribution of Corporate Data by Location
Source: Osterman Research, Inc.

## The Information on Your Smartphone or Tablet Can Be Easily Compromised

One of the fundamental problems with your mobile devices is the thing that makes them so useful: their mobility. This means that your smartphone and tablet contain sensitive or confidential corporate information that can create a data breach if they are lost or stolen. Here are a few examples of what can happen:

**Consumer Reports found that 4.5 million smartphones were stolen or lost in 2013, up dramatically from 2.8 million in 2012.[17]**

- In January 2016, New West Health Services in Kalispell, MT revealed that one of its laptops went missing, breaching 28,209 records.[3]
- An employee of Buyers Protection Group in Alpharetta, GA had a laptop stolen during a large-scale burglary of cars, revealing an unknown number of customer records.[4]
- Consumer Reports found that 4.5 million smartphones were stolen or lost in 2013, up dramatically from 2.8 million in 2012.[5]

In addition to the problem of theft or loss of mobile devices are the following issues that can result in data breaches and other problems:

- A growing proportion of mobile devices are personally owned—an Osterman Research survey conducted during January 2016 found that for 39% of employees, the primary work-related smartphone they use is their personally owned device.[6] This means that a substantial proportion of mobile devices—and the corporate data contained on them—is under the control of you and your fellow employees, not the IT department.
- Many users do not password-protect their personally owned devices or know how to delete all of the data from them if they are lost. An unprotected mobile device that cannot be wiped can result in a data breach if it is lost or stolen.

Even if the data has not actually been breached as the result of a loss or theft, the company whose data was lost must still report the breach depending on the type of data that was compromised. For example, loss of sensitive or confidential health care patient information in excess of 500 records must be reported to the U.S. Department of Health and Human Services, and 47 of the 50 U.S. states require reporting of any breach of unencrypted information to its owners in those states.

Many users are tempted to access publicly available Wi-Fi connections, particularly when using tablets or laptops that do not have a cellular connection. Public Wi-Fi hotspots, available at locations like coffee shops, airports and restaurants, are notoriously subject to hacking by cyber criminals. When users enter their login credentials to access corporate email, social media and other sensitive sites, hackers can easily steal these credentials to gain access.

Many users mistakenly download "copycat" applications to their mobile devices that allow cyber criminals to steal sensitive information. These apps are designed to look and operate like legitimate apps, but instead are intended for a variety of malicious purposes. For example, a developer can easily disassemble an existing app and repackage it so that it looks similar or identical to a legitimate one, but the app will include code that will add spam or other advertising in the app interface, send expensive SMS messages that will add charges to the victim's wireless bill, or implement a capability to steal login credentials. As just one example, NQ Mobile reported a copycat mobile app designed to impersonate the legitimate NetDragon 91 Assistant app. When installed, the copycat app sends premium SMS messages that will appear as additional charges on victims' wireless bills.[7]

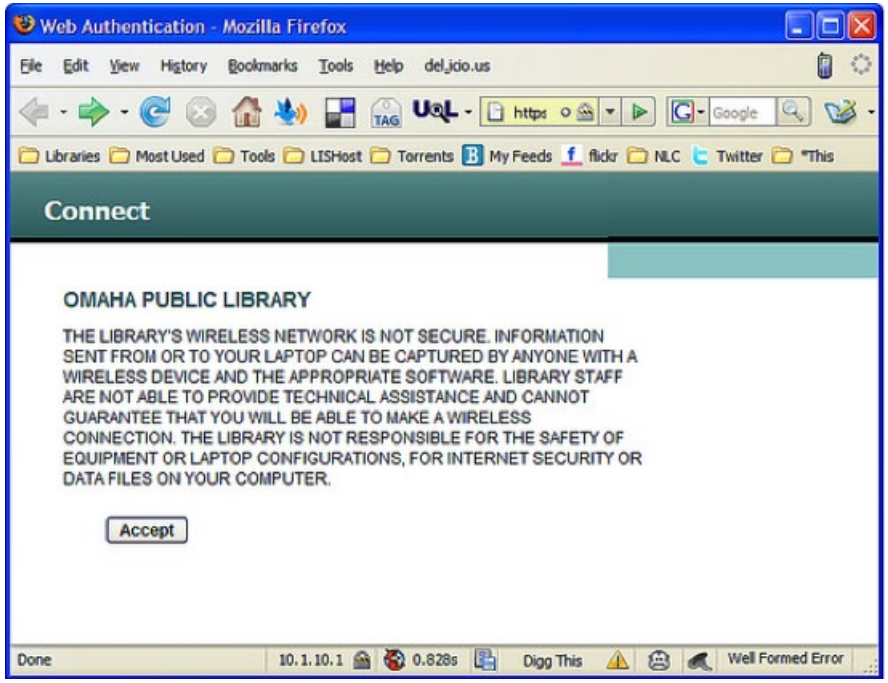


Figure 2: Public Wi-Fi Network Warning Message
Source: The Travelin' Librarian

## How to Defend Yourself

There are a number of things that users can do to mitigate the risks associated with the use of mobile devices when used for work-related purposes:

### USE PASSWORD PROTECTION

First and foremost, every mobile device you use should be password-protected so that any sensitive or confidential information stored on it will not be easily accessible.

### DISABLE AUTO USERNAME AND PASSWORD COMPLETION

You should disable automatic username and password completion. While this makes the use of a mobile device somewhat more tedious, it can reduce the likelihood of sensitive or confidential information being accessed by someone who finds or steals an unprotected mobile device.

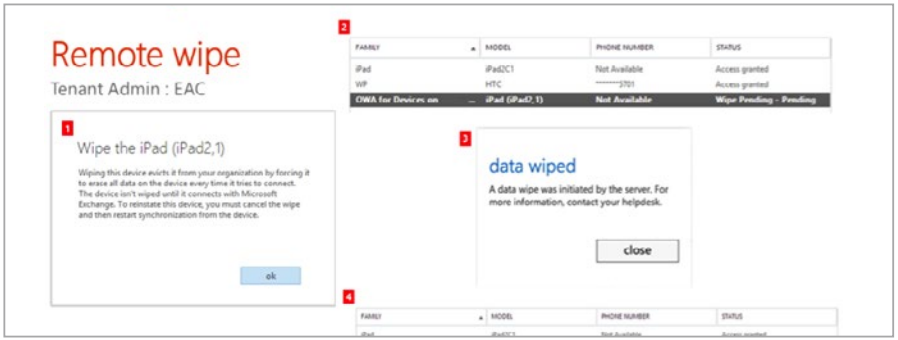


Figure 3: Tenant Admin Wipe Screen in Microsoft Exchange Admin Center
Source: Microsoft

### ALWAYS INSTALL SECURITY UPDATES

You should always elect to install updates—many of which are focused on improving security—as soon as they are available. A failure to do so can leave a mobile device more vulnerable to security threats than is necessary.

### BE SURE YOU CAN WIPE YOUR DATA

Ensure that your device can be wiped of all data if it is lost or stolen. While IT departments can generally do this for company-supplied devices, if you employ your own device you should know how to do this.

### BE VERY CAREFUL WHEN USING PUBLIC WI-FI NETWORKS

You should be very careful when accessing public Wi-Fi networks. Networks that do not require a password are highly insecure and even networks that require only a WEP password can be easily hacked. Wi-Fi networks that require the use of a WPA or WPA2 password are not invulnerable, but are much more secure.

### USE A HOTSPOT ON A TRUSTED PHONE OR AN ENCRYPTED VPN

If possible, when connecting a laptop or tablet to the Internet, you should employ a hotspot on a trusted mobile phone, or use an encrypted VPN when using a public Wi-Fi hotspot.

### DISABLE FILE SYNC AND SHARE

If you connect to any public network, disable all file sync and share tools, such as Dropbox, to reduce the likelihood of a data breach.

### BE CAREFUL WHEN ENTERING SENSITIVE INFORMATION

When you access a website that requires entering sensitive or confidential information, do so only on websites that are encrypted (i.e., the URLs begin with "https" and contain an icon of a lock in the URL bar).

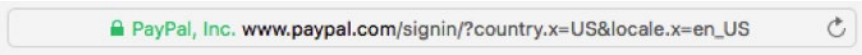


Figure 4: Example of an Authentic and Secure URL Source: PayPal

### USE ONLY "SAFE" STORES

When downloading mobile apps, use only stores with robust security controls, such as the Apple Store or Google Play. Many third party stores do not have rigorous security controls and can serve as a host to copycat or other malicious apps.

### SEE IF YOU CAN GAIN ACCESS TO SEGMENTATION TECHNOLOGIES

While you probably don't have control over technologies installed on a mobile device that can segment personal and corporate data on the same device, you can ask your IT department to at least investigate them. These technologies will permit the corporate "side" of the mobile device to be wiped by IT if the device is lost or stolen (or when an employee leaves the company), while not affecting your personal information.

## References

1 http://www.privacyrights.org/data-breach
2 Source: *CEB The Future of Corporate ITL: 2013-2017.* 2013.
3 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF4A0922D09B6E1CF5DAE375E0D0.ajp13w
4 http://oag.ca.gov/ecrime/databreach/reports/sb24-57473
5 http://www.latimes.com/business/technology/la-fi-tn-45-million-smartphones-lost-stolen-2013-20140417-story.html
6 Results of a *Survey of End Users' Messaging, BYOD and Social Media Practices,* Osterman Research, Inc.
7 http://securitywatch.pcmag.com/mobile-security/317083-mobile-threat-monday-malicious-banking-apps-and-crafty-copycats

Edition: 4.2116

## About ThinkHR

ThinkHR provides expert HR knowledge solutions designed to help people and companies thrive. Combining the best of human expertise and innovative technology, ThinkHR's solutions include the industry's first and most used HR hotline, an award-winning online HR knowledge base, and a comprehensive eLearning platform.

ThinkHR's mission is to give its partners a powerful competitive advantage to help them strengthen their client relationships, manage risk and win more business. Equally important, the company is passionate about empowering HR professionals and other executives to become more efficient, productive and successful.

For more information, visit thinkhr.com

**ThinkHR**
855.271.1050
contact@thinkhr.com

## About Osterman Research

Osterman Research provides timely and accurate market research, cost data, cost models, benchmarking information and other services to technology-based companies. We do this by continually gathering information from IT decision-makers and end-users of information technology through in-depth market research surveys. We analyze and report this information to help companies develop and improve the products and services they offer, and to help organizations make better decisions about their security, archiving and other capabilities.

For more information, visit ostermanresearch.com.





Edition: 4.2116