ThinkHR

Human Powered

# CYBERSECURITY PART 5: SOCIAL MEDIA

ThinkHR
Human Powered

# CYBERSECURITY PART 5: SOCIAL MEDIA

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 5 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]

# Social Media Is Another Big Problem

## Social Media Use Is Widespread

The use of social media in the workplace is pervasive, not only by employees for their own use, but also for legitimate business purposes. For example, 73% of the organizations surveyed by Osterman Research in January 2016 employ Facebook for business purposes, 64% use LinkedIn, and 56% use Twitter, in addition to a variety of other social media platforms.

## How Does Social Media Pose a Threat?

Social media can provide you with a number of important benefits that can help your company to become more efficient, help you to speed the decision-making process, and allow information to be shared in a way that is not possible or practical using other methods. However, the use of social media also represents a significant threat:

### HACKED ACCOUNTS

Many social media accounts are hacked by cyber criminals. For example, one source estimates that 160,000 Facebook accounts are hacked on a typical day.[2] Social media accounts can be hacked through phishing schemes, through the variety of third-party apps for which users give write access, or simple password cracking. The result of a hacked account may be nothing more than sending spam messages, or it can be part of a malware distribution campaign.

**Many social media accounts are hacked by cyber criminals. For example, one source estimates that 160,000 Facebook accounts are hacked on a typical day.**

### MALWARE DISTRIBUTION

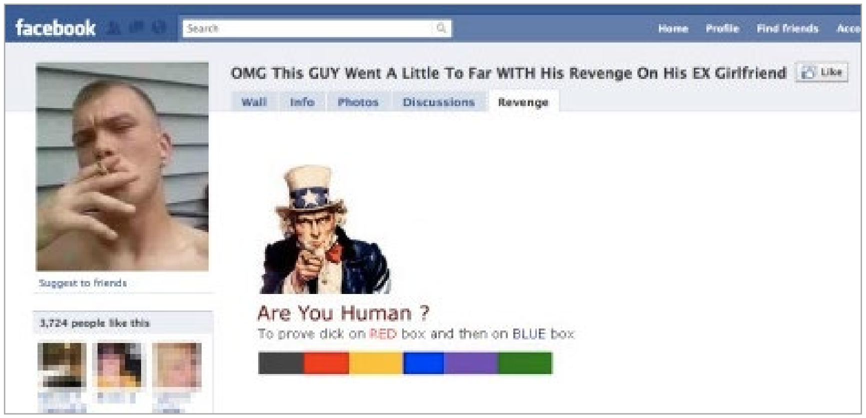
Social media platforms that limit the number of characters that can be sent, such as Twitter, necessitate the use of short URLs that can make it much easier for cyber criminals to disguise a link to a malicious site. Social media can also be the target of state-sponsored attacks. For example, in December 2015 Twitter issued a security alert to some users that they might have been “targeted by state-sponsored actors,” the first alert of its type made by the company.[3] Moreover, malvertising is on the increase and can infect leading social media properties. Proofpoint recently discovered a promoted Twittercard that can lead to installation of malware designed to steal Facebook credentials.[4]

### SCAMS AND BOGUS OFFERS

Social media is also a breeding ground for all sorts of scams and bogus offers that can trick users into revealing sensitive information. One study found that 24% of Facebook advertisements were selling counterfeit products.[5] As just one example, as of February 2016, Facebook had been hosting a bogus website for at least the past 15 months: the site for "South West Airline."[6] The Facebook page is clearly bogus, not only because it contains a URL for a domain that has not been registered, but also because the perpetrators of this fraud did not spell the name of the airline correctly. The page has been "liked" by nearly 3,000 people and it displays an offer that has been shared nearly 23,000 times.

### CLICKJACKING

This practice involves burying various hyperlinks under legitimate content on a social media page. When a user clicks on what he or she believes to be a valid link, the result can be a malware download to the computer or distribution of the link to other contacts after clicking the "Share" or "Like" button.[7]



OMG This GUY Went A Little To Far WITH His Revenge On His EX Girlfriend

Are You Human ?

To prove dick on RED box and then on BLUE box

Figure 1: Example of Clickjacking in Facebook

Source: Facebook

## The Biggest Problem Is Users

The core of the social media security problem is users who fail to be sufficiently skeptical of advertisements, too-good-to-be-true offers, or who are too willing to "like" or "share" posts. Add to this the problem of oversharing information on social media, thereby providing phishers and spearphishers with the information they need to increase their chances of success. For example, if you share your experience about XYZ Restaurant on Facebook and your profile is public, a cyber criminal can use this information to send you an email with the subject line, "Problem with your recent credit card charge at XYZ Restaurant." Given that you were there recently, it makes sense that you would receive an email of this type, making you more likely to open it. Moreover, sharing too much information via social media can allow others to "connect the dots" about a merger, acquisition or some other business deal that would not otherwise have been revealed.

# How to Defend Yourself

There are a number of things that you can do to increase the security of your experience and reduce the likelihood of malware infiltration, data loss or other problems:

### DON'T OVERSHARE

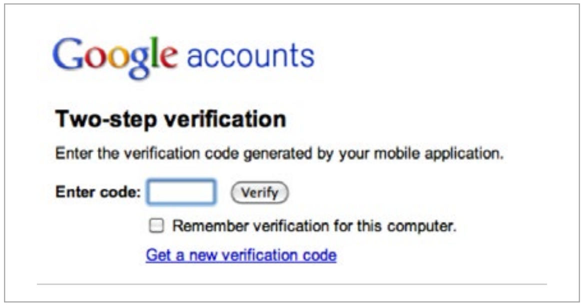
Simply put, don't share an excessive amount of information via social media. Not every dessert, vacation photo, medical condition or thought needs to find its way onto a social media page. Toward this end, it might be useful to limit who can see posts or access contact information on Facebook, Instagram and other social media properties. These controls are typically available in the settings of your social media account.

### TURN OFF LOCATION SERVICES

Many social media platforms permit you to share your location, either manually or through geolocation services that will automatically post your location. Use of location information in social media posts can tell business colleagues about your multiple trips to Bentonville, Arkansas (which could strongly hint that your company is about to do a deal with Wal-Mart, for example). In an extreme example of the dangers inherent in automatically sharing location data, some U.S. soldiers in Iraq posted photos on Facebook, not realizing that they had been geotagged. This provided insurgents with the data they needed to destroy four Apache helicopters.[8]

### TURN ON OUT-OF-BAND AUTHENTICATION

Many social media platforms permit the use of out-of-band authentication that will require entry of a code delivered to a mobile device when logging in from a new browser. This can reduce the likelihood that cyber criminals will be able to access your social media account.


Google accounts

Two-step verification

Enter the verification code generated by your mobile application.

Enter code: ▭ Verify

□ Remember verification for this computer.

Get a new verification code

Figure 2: Two-Factor Authentication in Google Apps
Source: Google

Many social media platforms permit the use of out-of-band authentication that will require entry of a code delivered to a mobile device when logging in from a new browser.

### BE CAREFUL WHEN CLICKING, LIKING OR SHARING

Finally, be careful when clicking on a link or sharing it. As noted, doing so could inadvertently distribute malware or spammy messages to others in your social media circle.

# References

1 http://www.privacyrights.org/data-breach

2 http://nypost.com/2015/03/01/big-brother-2-0-160000-facebook-pages-are-hacked-a-day/

3 http://www.databreachtoday.com/twitter-state-sponsored-attack-alerts-a-8746

4 http://www.techweekeurope.co.uk/e-marketing/malvertising-promoted-tweet-twitter-proofpoint-181879

5 https://www.scribd.com/doc/245368772/Counterfeit-Facebook-quantitative-analysis?secret_password=IO7mLskTLSCwSfrRTLNe

6 https://www.facebook.com/South-West-Airline-1542500652685286/?fref=ts

7 https://nakedsecurity.sophos.com/2012/05/08/facebook-clickjacking/

8 http://nypost.com/2015/03/01/big-brother-2-0-160000-facebook-pages-are-hacked-a-day/

## 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.

This document is offered for general best practice information only. It does not provide, and is not intended to provide, legal advice.

Edition: 4.2116