„Ante Portas – Studia nad Bezpieczeństwem”
2016, nr 2(7)

Mykola Prokhorov
Ukraine

SOCIAL MEDIA SECURITY RISKS AND COMMUNICATION SECURITY SYSTEMS

Summary:
The article reveals the idea that popularity of social networking sites has increased at astonishing levels. There is no arguing the usefulness of sites such as Facebook, Twitter and LinkedIn. They can be used for professional networking and job searches, as a means to increase sales revenue, as a tool to keep the public informed of safety and other issues or as a way to reconnect with friends from way-back-when. Social networking has changed the way we interact with friends and associates. While social networks, like Facebook, Twitter, YouTube, FourSquare, and Google+, play a significant role in our lives, they are also a high risk for security threats. With hundreds of millions of users online, these tools not only attract friends and family wanting to stay in touch, but they also attract people wanting to know about you for the wrong reasons. Be aware of the security threats currently out there to help you stay safe online. In Europe, concerns about privacy linked to security are particularly acute, as evidenced by proposals for a new cyber security directive that link privacy and security. The proposals aim to impose EU-wide reporting requirements on companies that run large databases, including social networking firms. Although the final wording of the directive remains to be seen, the proposals are a good indication of just how seriously European authorities view data security breaches.

Keywords:
social media, social networks, communication security, security risks, security systems

Social media is an unprecedented phenomenon that has opened new worlds of opportunity for organizations around the globe. While the potential and rewards are seemingly limitless, so are the challenges and risks. Savvy organizations are making it a priority to re-think outdated “Internet” policies to include social media, bringing significant changes to their security posture. Today the

lines between an individual's work persona and private persona are increasingly blurred. Forums, blogs, and popular social networks like Facebook, LinkedIn and Twitter are just the tip of the social media iceberg. The ubiquitous nature of smartphones and other mobile devices has made the "anywhere, anytime" Internet a reality, and sensitive company information is no longer confined to the limits of the corporate perimeter.

Social platforms are thriving, but so are schemes to use them for crime and ill will. Risks such as data leakage pose the biggest threat to most organizations. Social media "squatting" and sophisticated social engineering schemes are changing the landscape for security professionals, with consequences ranging from brand reputation damage and lost productivity to potential physical harm to employees and executives. There are proactive steps every organization can take to strengthen their security posture and minimize potential damage. Addressing these challenges effectively begins with a solid understanding of both the authorized and unauthorized social media users.

With social media now a part of daily life for millions of people around the world, the Internet is a far different place from the online world of even a few years ago. Gone are the days of static content on a website that changed slowly. Today, social media has turned the Internet into a thriving, "always on" environment of constant activity, near real-time postings, chats, tweets, and millions of video uploads to YouTube, Vine, and other popular platforms every minute.

The way people engage with the Internet has drastically changed as well. Social media has opened a world of constant "anywhere, anytime" access thanks to the abundance and popularity of smartphone devices such as the iPhone, BlackBerry, and Android. In fact, statistics from Pew Internet Project's research for mobile technology show that as of January 2014, 90% of American adults owned a cell phone and, 42% of American adults own a tablet computer[1].

There are more connected mobile devices on earth than the number of people. *No other technology has impacted us like the mobile phone. It's the fastest growing man-made phenomenon ever – from zero to 7.2 billion in three decades*, said Kevin Kimberlin, Chairman of Spencer Trask & Co.2 The majority of digital media is consumed with mobile applications, surpassing even desktop usage.3 In terms of social media, personal use of social networking applications accounted for an estimated 46% of all smartphone activity and 19% of all tablet traffic.

Social media platforms such as Twitter, Facebook and LinkedIn increasingly are being used by enterprises to engage with customers, build their brands and communicate information to the rest of the world.

But social media for enterprises isn't all about "liking," "friending," "upvoting" or "digging." For organizations, there are real risks to using social me-

[1] D. M. Boyd, N. B. Ellison, *Social network sites: Definition, history, and scholarship,* "Journal of Computer Mediated Communication", 2007, 13(1), pp. 210-230.

dia, ranging from damaging the brand to exposing proprietary information to inviting lawsuits.

According to the Cisco 2013 Annual Security Report, the highest concentration of online security threats is on mass audience sites, including social media. The report revealed that online advertisements are 182 times more likely to deliver malicious content than pornography sites, for example.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just as damaging.

The report's authors draw the analogy of shouting "Fire" in a crowded cinema. Within minutes, people can be trampled to death before a correction can be made to the message.

In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information.There have been several incidents over the past year where false information transmitted on the internet has had serious consequences, according to the report.

We now know that undesirable things happen in cyberspace. I he list that follows is not exhaustive as human ingenuity keeps developing new ways to exploit insecurity:

- Financial loss: in 1995 a British bank with a long history went out of business, then in 2008 a French bank lost over 6 billion Euro. In 2011 a Swiss bank operating in London lost 2 billion dollars. In the three cases through insider misuse or abuse. These were not unique situations.
- Denial of Service attacks – these overload a system, usually a website or an electronic mail service so that it cannot function. Such attacks are easy enough to carry out and are usually successful. Sabotage of networks or computer systems to interfere with their operation. Usage of malicious software to take control of a computer or computer system for any of many possible reasons[2].
- Theft of Intellectual Property – including industrial espionage. Theft of Personally Identifiable Information – a breach of privacy leading to impersonation. Corruption or destruction of corporate data or software – frequently using malicious software. Are the growing concerns about the threat of cyber attacks on critical infrastructures such as utilities (power, water, communications, transport, hospitals, etc.) as well as on law enforcement and emergency services. Politicians around the world have also accepted that there is a threat that entities playing a critical

[2] *2013 Cisco Annual Security Report*,
<https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf> (10.12.2016).

role in national security, such military facilities and operations in the field, may the target of a cyber attack.

A favorite of smooth-talking scammers everywhere, social engineering has been around since before computer networks. Social media has taken this threat to a new level for two reasons:

1. people are more willing than ever to share personal information about themselves online via Facebook, Twitter, Foursquare and Myspace;
2. social media platforms encourage a dangerous level of assumed trust. From there it's a short step to telling your new friend about your company's secret project. Which your new friend really might be able to help with if you would only give him a password to gain access to a protected file on your corporate network. Just this once.

Before digital social networking, social-engineering culprits were called confidence or "con" men. They typically committed fraud through human interactions, a technique that was limited by the number of people they could reach. Today's social engineers have gone digital. Phishing is an effective vector of attack, particularly when used in conjunction with social media, enables criminals to reach thousands of potential fraud victims. Targets of phishing attacks may unwittingly divulge usernames and passwords, credit card numbers, and other information that can be used for fraudulent purposes. In the workplace, phishing can lead to leakage of sensitive or regulated data, infect the network with malware, and provide ingress for advanced persistent threat, a tenacious criminal attempt to access information on an organization's computer systems.

As the use of social media rises, so do phishing expeditions: The Anti-Phishing Work Group reports that phishing attacks increased 58 percent during the first half of 2011 compared with the same period the year before. Adding to security concerns, phishing has become simplified and increasingly pervasive as traditional applications have been recast as mobile social media apps. Today, it is alarmingly commonplace for hackers to unleash malicious code on social media apps for smart phones. It is also very effective: Ponemon found that almost one in three (29%) security breaches result from malware borne by social media. Phishing, and the more targeted spear phishing, are also employed for sophisticated cyber crimes like APT.

Recent APT attacks have employed phishing email messages that infect computers after users open a file or click a bogus link. Often, social media sites provide the employee information that enables intruders to craft an effective spear phishing email. This tactic, for instance, is believed to have been employed by the perpetrators of "Operation Aurora," a coordinated cyber attack against Google and at least 30 other companies that was used to steal corporate intellectual property and gain access to user accounts. Another danger, particularly for Twitter users, is the use of abbreviated URLs. URL shortening services from sites such as Bit.ly and is.gd obscure the destination of the link from the

user, creating a particularly effective tool for cyber criminals. Indeed, Symantec reported that, during one three-month period, 65 percent of malicious URLs found on social networks were hiding behind shortened URLs[3].

A recent scam on Facebook, for instance, employed a shortened URL to lure users to a site to receive an iPad 2 for review. Not only did victims voluntarily surrender account information and personal data, they also infected their computers with malware. Another way to uncover user account information is the use of data-mining scripts that "scrape" information from social networking sites. Many people use the same log-in information for multiple social media accounts, and this information is tempting and potentially profitable to criminals. In late 2010, for instance, hackers compromised the servers of Gawker Media, a highprofile blog network, and obtained 1.4 million user passwords and other confidential information. The user information was posted on a public torrent, and within a matter of days spammers used the e-mail addresses and passwords lifted from Gawker's servers to take control of Twitter accounts. Not all information leaks result from the efforts of criminals, however. Employees themselves may voluntarily disclose critical business information and intellectual property. As we have seen, many users post to social media sites from work, and they can inadvertently disclose sensitive business information such as confidential details about a software project or a new product under development. Use of location-based social networking apps also can unintentionally provide information that can be exploited by competitors. For instance, an employee who broadcasts his or her whereabouts by "checking in" to locations using Foursquare might compromise an acquisition if the employee repeatedly checks into the target company's location during negotiations In addition to personal and business information, data leakage also can violate confidentiality mandates. For instance, we have seen numerous cases in which a healthcare employee posted information about a patient's medical records on social media, a clear violation of the Health Insurance Portability and Accountability Act. The practice may be more common than you think: A study by Websense found that 20 percent of IT managers reported they had seen confidential information posted on social networking sites[4].

Social networking has changed the way we interact with friends and associates. While social networks, like Facebook, Twitter, YouTube, FourSquare, and Google+, play a significant role in our lives, they are also a high risk for security threats.With hundreds of millions of users online, these tools not only attract friends and family wanting to stay in touch, but they also attract people

[3] G. Pallis, D. Zeinalipour-Yazti, M. D. Dikaiakos, *Online Social Networks: Status and Trends. New Directions in Web Data Management 1,* "Studies in Computational Intelligence", Volume 331, 2011, pp. 213-234.

[4] J. Weizenbaum, *ELIZA – a Computer Program for the Study of Natural Language Communication Between Man and Machine,* "Communications of the ACM", 1966, Vol. 9, No. 1, pp. 36-45.

wanting to know about you for the wrong reasons. Be aware of the top five security threats currently out there to help you stay safe online.

Having Your Identity Stolen. Identity thieves gather personal information from social media sites. Even if you have your account on the highest security settings, there are still ways for an identity thief to get your information. Most social network sites have information that is required, such as email address or birthday. It's common for an identity thief to hack an email account by using social information. For example, a common technique to get personal information is by clicking on "forgot password" and trying to recover the information through email. Once the thief has access to your email account, they then have access to all information on your social networking sites.

So what can you do to protect yourself? You don't have to delete all your social profiles or hide from the real world; just take these precautions.

Have a strong password. The stronger your password, the harder it is to guess. Use special characters like symbols and capital letters when creating your password. Also, don't use "common" passwords, like your birthday or your child's name.

Be careful with your status updates. Often, we innocently post status updates that would give an identity thief information they need to steal our identity. For example, you may post *Happy birthday to my mother!* and then tag her in the post. Likely, your mother's maiden name will be associated with that tag now. A popular security question is *What is your mother's maiden name?* and if you share that online, you run the risks of identity thieves getting the answer to this commonly used question.

Don't reveal your location. You can use a fake location or make one up from another city and state. You may even be able to leave this information blank. Be cautious and never use a city and state where you live.

Getting Your Computer Or Social Profile Hacked. Hackers love social networking, going right to the source to interject malicious code. The codes hackers use can steal your identity, inject viruses to your computer, and obstruct bank account information, to name a few. Shortened URLs, such as those created on bit.ly, are especially susceptible to hackers. Shortened URLs can trick users into visiting harmful sites where personal information can be compromised because the full URL is not seen. The best advice is to never click on a link until you are sure of the source. To tell if a link is safe, you can: Hover over the link. If you hover over a link without clicking, you'll see the full URL in the lower corner of your browser. If this is a website you recognize, go ahead and click.

Try a link scanner. A link scanner is a website that lets you enter the URL of a link you suspect might be suspicious to check for safety. Try URLVoid or MyWOT as possible options.

Check shortened links. A shortened link is popular on sites like Twitter where character length matters. Some shortened link sites include bit.ly, Ow.ly, and TinyURL. Use a service like Sucuri to determine if the real link is secure[5].

Inadvertently Letting Stalkers Find You. When you use social networking sites, you are posting personal information. Once information is posted online, it's no longer private and can fall into the wrong hands. The more you post, the more vulnerable you become to those who may wish to harm you. Even with the highest security settings, friends, associates, and even the brands you "like" on your networking sites, can inadvertently leak information about you. The websites you subscribe to, the apps you download, and the games you play on social networking sites all contain personal information about you. Every time you browse a website, companies can put invisible markers on your computer called cookies. In theory, no two cookies are alike. When you are online, these cookies track your activity as you move from site to site.

To keep sites from tracking your activity, click on the "Do Not Track" feature. Most websites have an option for you to opt out of tracking. You can also clear the cache and cookies on your browser regularly to help prevent any problems.

Letting Burglars Know Your Whereabouts. Telling the online world where you're going and when you aren't at home is inviting burglars to your house.Did you know that a run-of-the-mill burglar can break into your home in less than 60 seconds and spend less than 10 minutes stealing your possessions? By telling the world you are on vacation in Europe, you're letting potential thieves know where you are, how long you'll be gone, and where you live. Burglars are fond of constant updates, especially about your travel plans. You wouldn't stand up in the middle of a crowd and announce you're going on vacation for a week, would you? Of course not, but that's what you do when you post your vacation pictures and plans online.

When you go on vacation: Avoid posting specific travel plans. Never post when, where, or how long you'll be gone. Wait until you are home to post pictures to a vacation album. Use highest privacy control. Only let certain groups, like a family group, view your photos. Be selective with the status updates. You can use an audience-selector dropdown menu on Facebook to choose certain groups to see your status updates.

Stay offline. You're on vacation, after all. Relax and forget about the online world for a few days.

Becoming overconfident. One of the biggest threats to online security is overconfidence. Whether at home or at work, many users believe as long as they have a firewall and an antivirus installed, there is no threat to security. Many people also believe that they don't have anything worth hacking so there's no need to worry about security. With today's technology, we are more

[5] A. N. Ayofe, B. Irwin, *Cyber security: challenges and the way forward*, "Computer Sciences and Telecommunications", 2010, No. 6, pp. 56-69.

connected to each other than ever before. When you neglect security, you not only put yourself at risk, but others are at risk as well[6].

To keep yourself and your information safe, pay careful attention to your online activity. Avoid posting information including: travel plans, bank account information, your full address and birthdate, your children's' names, school, and birthdates, location information, such as the name of your work place, your daily schedule.

You can still use social networks for all they were meant to accomplish, but you need to take extra precautions to make sure your personal information doesn't get in the wrong hands. Know what threats you are most vulnerable to and take steps to protect yourself and your networks.

Computer security with regard to system security and network security has been broadly studied. With the development of multimedia processing and applications, multiple types of media security have been broadly taken into consideration. The type of media includes audio, video, image, text, web pages and graphics.

From a hardware perspective, in order to protect the copyright of Intelligent Property (IP), special fonts were written into the ROM on microchips so that fraudulent chips could be identified. If these marks are removed, the fragile microchip will no long function. This technique has been employed even today, the microchip protections are still regarded as one of the best ways to protect information pertaining to that chip. Another typical software protection is a "serial number", which attempts to block illicit copying, along with online Internet registration of that software.

Visually, logos have been adopted as a type of visible watermark, used frequently within the television industry. These marks are used to denote content ownership.

Nowadays, secure protection approaches have been embedded into the commercial products such as computer games, digital music, digital video, engineer's drawings and many other forms of digital media and documents. Duo to the rapid expansion of the amount of digital content available, illegal usage of these products can have many detrimental effects. It cannot be denied that media security will play a vital role in the impact multimedia products will have over a long period of time.

Alt hough the research in the area of media security has made great progress in the past ten years, there are still many problems with existing products and additionally, during that time, many more problems, previously not considered have presented themselves. The robustness and capabilities of the existing security models have not been sufficiently investigated or updated to handle these new problems.

---

[6] D. L. Speer, *Redefining borders: the challenges of cybercrime*, "Crime, Law and Social Change", 2011, T. 34, No. 3, pp. 259-273; J.L. Sternberg, *Misbehavior in cyber places: the regulation of online conduct in virtual communities on the Internet*, Lanham 2012.

BIBLIOGRAPHY:

Books and articles:

- ✓ Ayofe A. N., Irwin B., *Cyber security: challenges and the way forward*, "Computer Sciences and Telecommunications", 2010, No. 6
- ✓ Boyd D. M., Ellison N. B., *Social network sites: Definition, history, and scholarship*, "Journal of Computer Mediated Communication", 2007, 13(1)
- ✓ Pallis G., Zeinalipour-Yazti D., Dikaiakos M. D., *Online Social Networks: Status and Trends. New Directions in Web Data Management 1*, "Studies in Computational Intelligence", Volume 331, 2011
- ✓ Speer D. L., *Redefining borders: the challenges of cybercrime*, "Crime, Law and Social Change", 2011, T. 34, No. 3
- ✓ Sternberg J. L., *Misbehavior in cyber places: the regulation of online conduct in virtual communities on the Internet*, Lanham 2012
- ✓ Weizenbaum J., *ELIZA – a Computer Program for the Study of Natural Language Communication Between Man and Machine,* "Communications of the ACM", 1966, Vol. 9, No. 1

Internet sources:

- ✓ *2013 Cisco Annual Security Report*, <https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf> (10.12.2016)