



IBM Center for
The Business of Government

Strengthening
Cybersecurity Series

A Best Practices Guide for Mitigating Risk in the Use of Social Media



Alan Oxley

Universiti Teknologi PETRONAS
Malaysia

A Best Practices Guide for Mitigating Risk in the Use of Social Media

Alan Oxley

Professor
Computer and Information Sciences Department
Universiti Teknologi PETRONAS Malaysia

TABLE OF CONTENTS

- Foreword** 3
- Executive Summary** 4
- Introduction** 5
 - Background 5
 - How We Participate and Collaborate Online 6
 - The Potential—and Potential Risk—of Social Media 7
 - Relevant Security Threats 8
- Mitigating The Risk of Identity Theft**..... 9
 - Information Scraping..... 9
 - Social Engineering 12
 - Phishing 14
 - Spoofing 18
- Mitigating the Risk of Malware**..... 20
 - E-mail Attachments 20
 - Social Media Websites 22
 - Unsecured Data Storage Devices 25
- References** 27
- About the Author** 30
- Key Contact Information**..... 31

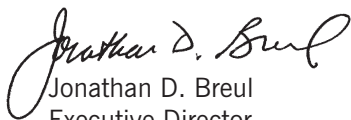
On behalf of the IBM Center for The Business of Government, we are pleased to present this report, *A Best Practices Guide for Mitigating Risk in the Use of Social Media*, by Professor Alan Oxley.

Social media continue to grow across the globe, and the United States federal government is no exception. The administration and Congress actively and increasingly use social media to communicate, to take information in, and to collaborate across boundaries. Yet the benefits of increased involvement through social media also raise new risks to the security of agency information.

This guide was written to help government managers, IT staff, and end users understand the risks they face when turning to social media to accomplish agency missions, and to mitigate those risks. The guide follows the publication of several other recent IBM Center reports which examine the current and potential use of social media by government agencies, including:

- *Assessing Public Participation in an Open Government Era* by Carolyn J. Lukensmeyer, Joseph P. Goldman, and David Stern
- *Using Wikis in Government: A Guide for Public Managers* by Ines Mergel
- *Using Online Tools to Engage—and be Engaged by—The Public* by Matt Leighninger

This guide complements these reports, presenting a view of the cybersecurity risks intrinsic to social media use and, more important, how to mitigate them. We hope that its suggested risk mitigation activities inform government agencies on how best to leverage social media in accomplishing their missions more effectively and efficiently—and more securely.



Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
jonathan.d.breul@us.ibm.com



Dar Chenok
Senior Fellow, IBM Center for The Business of
Government
IBM Global Business Services
chenokd@us.ibm.com

This guide explores how security controls can be used by government information technology staff, managers, and users to mitigate the risks intrinsic to social media. Specifically, this guide seeks to help readers understand the risks posed by many Web 2.0 applications and how best to mitigate those risks. Throughout the text, the term “government” refers to federal, state, and local government.

Cybersecurity is a complex topic. Social media have vulnerabilities, as do all computer applications. Some of these are specific to certain websites or applications, while others are intrinsic to all social media. The goal of this guide is to suggest hardware and software controls and acceptable use policies (AUPs) that mitigate risk.

The extent to which social media should be used in government depends on the likely benefits and potential risks—a determination that government managers must make. Government managers should place a high priority on the security of their digital assets, computer networks, staff, and constituents. They will have to decide whether or not there is a business case for the use of social media in their individual organizations. A risk assessment is inherent in the decision.

This guide describes the security measures that can be applied in the context of Web 2.0 social media applications. The guide covers two topics: identity theft, which is a threat both to government employees and the constituents they serve, and malware, which is a threat to computers and computer networks.

This guide presents risk mitigation activities for four identity theft threats: information scraping, social engineering, phishing, and spoofing. The guide also presents risk mitigation activities for three malware threats: e-mail attachments, spoofing, and unsecured data storage devices.

BACKGROUND

In January 2009, President Barack Obama issued a memorandum on the subject of transparency and open government, calling for transparency, participation, and collaboration (Obama, January 2009). Technological advances, especially those related to social media, have the potential to bring about a greater engagement by the public in government. Government's interest in using social media is growing rapidly, encouraged by administrators, politicians, and the general public.

Governments should implement strategies to motivate citizens to become active. Public involvement in society is desirable in democracies, and Web 2.0 is one way to achieve it. A main benefit of increased public involvement is increased public service efficiency with a consequent reduction in cost. A social network also has the potential value of building social capital.

As far as formulating U.S. technology policy is concerned, a conference was held in 2008—*Computers, Freedom, and Privacy: Technology Policy '08*—to discuss cybersecurity issues. Its organizers drew attention to the fact that “In the areas of privacy, intellectual property, cybersecurity, telecommunications, and freedom of speech, an increasing number of issues once confined to experts now penetrate public conversation” (Computers, Freedom, and Privacy Conference, 2008).

This guide addresses the cybersecurity measures, tools, and approaches that can enhance national, agency, and individual security (Bertot et al., August 12, 2010). The issues to be discussed are fundamental to the successful adoption of social media by government.

HOW WE PARTICIPATE AND COLLABORATE ONLINE

Participation and collaboration are facets of self-governance, and the tools we use to participate and collaborate are shaped by (and in turn shape) the relationship between collaborating parties. The primary vehicle for participation and collaboration is sharing: information, perspectives, tasks, and even resources. In discussing social media, there are four broad ways in which sharing can take place (Drapeau & Wells II, April 2009):

- 1. Inward sharing**, or sharing information within agencies. This type of sharing is restricted to government officials and excludes the public. Proprietary software exists for this, such as SharePoint and the micro-blogging service Yammer.
- 2. Outward sharing**, or sharing information with entities beyond agency boundaries. Examples of this type of sharing are GovLoop and STAR-TIDES. GovLoop is a social network for the government community which is not run by the U.S. government. STAR-TIDES is an acronym for Sharing To Accelerate Research—Transformative Innovation for Development and Emergency Support, a DoD sponsored knowledge-sharing research project that promotes sustainable support and humanitarian assistance to stressed populations across the world.
- 3. Inbound sharing**, also called crowdsourcing, allows government to obtain input from citizens and other persons outside the government more easily. One kind of crowdsourcing task is online voting, but there are several others. Two experiments in crowdsourcing are the Obama administration's SAVE awards, which requested ideas on how to streamline the U.S. government, and the House Republican website "America Speaking Out," which requests ideas from Americans on how to balance the budget and reduce the deficit.
- 4. Outbound sharing**, whose purpose is to communicate with and/or empower people outside the government. This can be achieved by web conferencing. A control group experiment to evaluate the acceptability and effectiveness of holding online town hall meetings was conducted in 2009 (Lazer et al., 2009). One finding: "Participants in the sessions were more likely to vote and were dramatically more likely to follow the election and to attempt to persuade other citizens how to vote."

THE POTENTIAL—AND POTENTIAL RISK—OF SOCIAL MEDIA

This guide provides advice on the security issues relating to the use of social media. Social media usage has the potential to enable U.S. citizens to participate more fully in government. It has already played a significant role in some of today's dramatic events.

Throughout the world, the public can use social networking websites to voice objections about their governments' plans. At a more extreme level, social networks have played a role in organizing protests that have brought down national governments. In the January 2011 protests in Egypt, social networking was credited with being a key mobilizing force. Facebook, a social networking website central to Egyptian protestors, has also been reported as being instrumental in the February 2011 social unrest in Bahrain. At the end of April 2011, it was widely reported that a Facebook page entitled "Syrian Revolution 2011" called for mass demonstrations after Friday prayers. Also in late April 2011 in Vietnam, Nguyen Cong Chinh was arrested, allegedly due to his anti-government stance, partly expressed through web posts (Viet Nam News, April 29, 2011).

Leaving these sensational examples aside, social media can allow people to interact in a more prosaic way with their elected leaders and know that the leaders themselves are listening. For example, David Plouffe, senior advisor to the president, monitors social networking chatter for Barack Obama (Scherer, May 30, 2011), an activity termed "sentiment analysis." Plouffe follows what is happening on Twitter and Facebook. On Twitter, the hashtags used to identify the topic of a tweet (for example, #immigration) allow all those who follow the specific topic to view the tweet.

Social media, however, also present a variety of new threats posed by cybercriminals and foreign partners. For example, when people use a social media website, they do not know how vulnerable the website is to security breaches. Furthermore, there is the problem of social engineering, a term used when someone is trying to fraudulently acquire confidential personal information from a user. Another problem is that social media websites also allow users to run third-party applications such as games and provide tools to personalize their page, and these uses have vulnerabilities.

RELEVANT SECURITY THREATS

Government information systems are a constant target of attacks from malicious individuals. There are a variety of threats, but most that are perpetrated through social media fall into one of two types: identity theft and malware.

Mitigating the Risk of Identity Theft

Identity theft is a crime that may occur to individuals or groups as large as hundreds of thousands of people at a single time. The damage may be as little as the loss of a hundred dollars (usually borne by financial institutions, in the case of stolen credit or debit cards) or hundreds of thousands of dollars in the case of fraudulently opened bank, credit, or even mortgage accounts; resulting in more losses from the legal work that must be done by both financial institutions and individuals to achieve resolution and restitution. To mitigate this risk, it is essential to understand how identity theft is perpetrated. Identity theft can occur by information scraping via social media websites and social media applications; social engineering; phishing; and spoofing.

Mitigating the Risk of Malware

Malware is short for “malicious software,” and covers a range of threats, including viruses, worms, trojans, bots, and other harmful code. Hackers develop malware for a number of reasons, including the desire to cripple the government or simply the potential of personal gain. Some malware is designed to attack the system in which it is installed; other forms are intended to take over their host system to launch an attack on a third party; and yet other applications are written not to cause any damage to the system, but to enable the creators to steal data residing on that system.

Whatever the goal of the malware, there are steps that end users, managers, and technical staff can take to mitigate the risk of malware. The point of attack determines the best countermeasures. The three most common sources for malware are e-mail attachments; websites, including social media websites; and unsecured data storage devices, such as thumb drives.

INFORMATION SCRAPING

Understanding the Risk

People put an astounding amount of personal information online: a phone number on one website, a picture on another, a birthdate on a third, an address on a fourth, and so on. What they fail to realize is that this information can be harvested or “scraped” from many websites and compiled into a single, comprehensive portrait of the user. This information can then be used by cybercriminals either to commit identity fraud or to sell to organizations who will commit identity fraud.

Why Social Media are Vulnerable

Social media websites are especially tempting targets for information scraping. There are two ways that this can happen. The first way is simply through accessing a person’s information page. Often, people will divulge information through a social media website, and then relax their privacy controls. Thankfully, this is easy to correct.

Social media websites also allow users to personalize their pages and to run third-party applications such as games. However, this grants the application access to all of a user’s personal information, irrespective of any privacy setting made in the social media website (Thomas et al., 2010). The vast majority of these applications only need basic personal details of a user. Furthermore, anyone can write an application and so some applications will have no security controls. Worse still, an application could have been developed by a cybercriminal.

Risk Mitigation Activities

Both managers and end users can help mitigate the risk of information scraping by creating and then following prudent social media guidelines. Though the specifics will be different for each office, the guiding principle is the same: don’t put any more personally identifiable information (PII) online than is strictly necessary.

To protect citizens who are accessing government services or communicating with their government online, management and IT staff must work together to ask for the least amount of personally identifiable information possible from citizens, and either delete that information once it is no longer necessary or safeguard it against possible theft.

By users

- Set privacy settings to their maximum, so that only trusted sources have access to personally identifiable information.
- Review all changes to the privacy policies of frequently visited websites, including social media websites.
- Carefully review the permissions requested by social media applications, including games and other add-ons requested by friends.
- Never divulge more personal information than absolutely necessary on any website. Personally identifiable information includes:
 - Tagged photos
 - A social security number (even a partial number)
 - Full name
 - Full date of birth
 - Schools attended
 - Work address (and phone number)
 - Family photos
 - The names of children and family members
 - Home address (and phone number)
 - Places regularly visited
 - Dates and details of future outings and vacations, and other times that the user will be away from home

By management

- Create an acceptable use policy (AUP) specifying the rules of behavior when using social media. Among other things, this should inform employees and the general public what information can and cannot be posted on the social media website.
- Stay abreast of proposed configuration changes to social media websites.
- Decide how long social media messages are to be retained.
- Respect the privacy of users from the general public. This applies not just to government data, but to data hosted by the social media provider.
- Periodically warn citizens of the threat of identity theft from information shared on social media websites. Additionally, managers should share the link to their official guidelines on what information should and should not be shared through social media.
- Create a process to handle unauthorized or fraudulent postings.

By IT staff

- Ensure that all websites are compliant with management guidelines.
- Update all security patches as required.
- Research ways to serve constituents without requiring them to divulge personally identifiable information.

SOCIAL ENGINEERING

Understanding the Risk

Social engineering is a method used by hackers to acquire confidential personal information through fraud. Sometimes the hacker will contact the victim directly and try to solicit personal information over the phone, through a web-based application like e-mail, or through a social media website. Another tactic is for a hacker to contact a third party, like an office administrator, executive assistant, or even IT staff. The hacker may ask for personally identifiable information such as birthdates, home or work addresses, or other data.

Why Social Media are Vulnerable

Managers, IT staff, and end users alike must recognize that connecting with people online poses privacy and security risks. One form of social engineering occurs when a cybercriminal on a social media website tries to befriend others. The intention is to build up trust so that confidential private information can be more easily extracted. The cybercriminal can create a fake Facebook profile or a bogus Twitter account.

On social media websites there are difficulties in establishing the authenticity of a person's identity when communicating with them, and in determining the accuracy of posts. Social media providers may be ineffective at detecting compromised accounts and subsequently restoring them. Another cybercriminal ploy is to try to befriend someone by claiming to have something in common; the cybercriminal may then contact the person through e-mail, over a social media website, or even on the telephone.

Risk Mitigation Activities

Social engineering relies primarily on person-to-person contact, bypassing many technical security measures. Because of the focus on individuals, the precautions fall mainly to end users and management, though IT staff may play a supporting role for each.

By users

- Never reveal personally identifiable information (PII)—whether through e-mail, a social media website, or even a phone conversation—unless certain of the recipient's credentials.
- Review and follow management's guidelines for interactions with constituents and IT administrators to protect all parties' PII.

By management

- Create a set of guidelines for sharing PII that encourages users to:
 - Understand the kinds of information that may be shared, and whom it may be shared with. This includes personal information about individuals.
 - Be cautious divulging their private information.
 - Appreciate the risks and understand the methods of social engineering.
 - Realize the legal issues involved in social engineering.
 - Attend training programs at regular intervals.

By IT staff

- Conduct training sessions at regular intervals and perform spot-checks to ensure compliance with social engineering rules.
- Ensure that systems are in place to help users guard against social engineering attacks.

PHISHING

Understanding the Risk

When social engineering is done via e-mail or social media website, it is referred to as phishing. The messages could be sent indiscriminately, or target an individual or a specific group. In the latter case, the practice is referred to as spear phishing. When the individual or group is a powerful one, the term whaling is used.

Phishing using social media messages raises additional security implications as these messages are not subjected to the checks performed by e-mail systems. Many web browsers do, however, have a phishing filter in them. The filter helps detect suspicious websites by comparing a website against a list of known rogue websites, and by checking to see whether a website fits the profile of a phishing website.

Why Social Media are Vulnerable

A message is more likely to be taken seriously if it contains information about the receiver. This information could be publicly available, as on a social media website, or it could be stolen.

The more the message is tailored to the receiver, the easier it is to pass through systems that filter out spam and messages with virus links or attachments, as the messages do not fit the pattern of typical rogue communication. There are also many scams, such as an e-mail asking for money because the presumed sender (a trusted person whose e-mail has been hacked) is stranded somewhere.

It is also conceivable that phishers could try to use a government agency as a cover for their scam, forging a “.gov” domain for their e-mail. Thus, in addition to guarding against internal employees falling prey to a phishing attack, government managers should be vigilant against fraudulent use of their agency domain.

Risk Mitigation Activities

Phishing can be countered both through technological and behavioral approaches.

By users

- **Social Media Websites**

- Join only those social media websites with explicit and strong privacy policies. Not all social media websites' privacy policies fully protect users' personally identifiable information. Several social networking websites allow non-registered individuals to view a profile, and others share users' e-mail addresses and preference information with third parties.

- **Account Settings**

- Frequently check the available privacy options to ensure that personal information is private. Use the "How others see you" tool on the [ReclaimPrivacy.org](https://www.reclaimprivacy.org) website to check that the privacy settings are functioning as expected. ([ReclaimPrivacy.org](https://www.reclaimprivacy.org) provides a tool that can be used to inspect a user's Facebook privacy settings, and give warnings about settings which make the user's information public.)
- When available, configure privacy settings so that only trusted individuals have access to posted information. Restrict the number of people who can post information on a personal page.
- Have a setting that will limit access to account data to protect it from an undesirable audience, as well as limiting access to your profile to family members, friends, teammates, or personal acquaintances.

- **Personal Information**

- Publish only the information necessary to maintain communication with other social media users.
- Ask "what personal information about me do I wish to be available online?" (Once information is online, it is no longer private. Individually, personal facts can seem to not pose a security risk; collectively, these personal facts constitute an individual profile.)
- Consider the type of information to be posted. For example, do not publish credit card numbers, financial account numbers, or confidential workplace information. Even birthdate information, coupled with a zip code, is often enough to identify someone.

- Remember the importance of personal privacy, either while creating profile information or posting information on a social networking website.
- Use only private messages (if available) to send personal or sensitive data to responsible persons. Sending sensitive data through social networking websites is not advisable, however, as it is not possible to be sure of the security protection on these websites.
- Post only general information that you are comfortable sharing with any social networking website member.
- Do not divulge certain information pertaining to plans, hopes, and goals. This information is often used by social engineering schemes.
- When uploading a photo, remember to take advantage of security measures that prevent others from copying and making use of the photo. (Before downloading a picture, a user should have concern for the owner of the picture and seek permission to download it, where necessary.)
- Do not publish private information about other people or the workplace.
- Divide friends into different lists, such as “Family,” “Friends Outside of Work,” “Colleagues,” etc. (A different level of access can be given to each list.)
- **Building up a Relationship**
 - Exercise caution when adding a previously unknown ‘friend’ or joining a new group or page. Before admitting a new person behind a privacy wall, whether a friend-of-a-friend or someone suggested by the social media website, attempt to confirm details about this new person. Find out their relationship to another trusted friend, perform a web search for the person, or use some other way of finding out more about the person.
 - Be conscious of behavior while on a social networking website. Remember to go through the above steps in order to avoid any unpleasantness. (Getting to know people in a virtual environment has many hazards. Although it can be rewarding, such interaction also carries significant risk. The above steps only suggest ways of countering some threats and do not necessarily prevent threats from materializing.)

- **Screen Names**

- Choose a screen name (identifying online pseudonym) that does not reveal too much personal information.

By management

- Prepare a guideline and training sessions for end users and technology staff on the dangers of phishing and how to handle suspicious e-mails.
- Develop a section of the agency's website—with a single point of contact—to help citizens verify that an e-mail purportedly sent by your agency is not the product of a phisher.
- Send information to the general public at regular intervals, reminding them of the existence of individuals who are trying to fraudulently acquire information, and the guidelines on what information should and should not be posted using social media.

By IT staff

- Use tools to monitor user behavior so that a check can be made on whether policy is being adhered to.
- Request the social media website owner to remove certain fields from a government user's page so that the user cannot give out personal information, such as a resume, through the page.
- Make users aware of the risks involved and give them examples of the types of attack.
- Make users aware of the acceptable use policy (AUP).
- Train users in the safe usage of social media websites.
- Make users aware of what information can be shared and with whom. This includes personal information about individuals.
- Caution users about divulging private information.
- Inform users about social engineering.
- Make users aware of the legal issues.
- Repeat awareness development and training at regular intervals.

SPOOFING

Understanding the Risk

The term spoofing refers to the practice of developing a website that mirrors a trusted website, but can be used either for identity theft—typically by asking users to send login information for the duplicated website—or to install malware onto the user’s computer. Spoofing can be accomplished in two ways: first, by sending a link in an e-mail or social media message; second, by hacking a trusted website, changing its behavior in a way that most users would not notice.

E-mail spoofing. Clicking a link in a message could cause a malicious webpage that installs malware to be displayed. The webpage sends malicious script to the user’s browser. When this happens it is referred to as a drive-by download. It is possible to get a rough idea of where the link is taking a user by looking at the URL. Note that the link that you see does not necessary take you to that address. To see where the link is taking you, you have to position the mouse cursor over the link. Furthermore, there are services which will take a URL and rename it. This is particularly useful in Twitter posts where the number of characters is limited. TinyURL and bit.ly are examples of URL shortening services. Developed to replace long URLs with short ones, they can also be used by malicious individuals to obscure the actual URL.

Website spoofing, including social media websites. Even if the website is a legitimate one, it may have been compromised with malicious scripts that will be downloaded to the user’s browser when the webpage is displayed.

Two examples are cross-site scripting (XSS) and cross-site request forgery. Cross-site request forgery is similar in operation to XSS, but allows a hacker to send unauthorized messages to the genuine website accessed by the victim.

Why Social Media are Vulnerable

The hyperlink that appears in a message may not necessarily lead to that address; it may redirect visitors to a fraudulent website that tricks users into revealing PII. Furthermore, it may take visitors either to a malicious website or a legitimate website that has been compromised. The fact that the initial URL is presented to visitors within the context of a trusted venue—whether e-mail or a social networking website—may add a false sense of legitimacy.

Risk Mitigation Activities

By users

- Do not click on unsolicited messages. Exercise the same caution with messages received via social networking as with unsolicited e-mails. Messages offering gifts are often fraudulent and may trick users into revealing personal information.
- Think carefully before clicking on a link, particularly if it is a shortened URL. If the sender of the link is known, they could be asked to confirm that the link is a legitimate one. URL shortening services usually have a mechanism through which the full URL may be viewed before using it. For example, for TinyURL service, simply enter `preview.tinyurl.com/LINKNAME`.
- Consider manually entering a URL rather than following a link.

By management

- Ensure that spoofing is covered in the organization's AUP.

By IT staff

- Use the government's own services, go.usa.gov and 1.usa.gov, to shorten a URL and mitigate the potential vulnerabilities associated with shortened URLs.
- Make users aware of the risks involved and give them examples of the types of attack.
- Make users aware of the AUP.
- Train users in the safe use of social media websites.
- Make users aware of relevant legal issues.
- Repeat awareness development and training at regular intervals.

E-MAIL ATTACHMENTS

Understanding the Risks

Files can be attached to an e-mail message. Similarly, files can be attached to social media messages, such as in Facebook. Attached files could be malware. Once again, the receiver is more likely to open the file if the filename is relevant to the receiver. For example, if an employee of the IBM Center for The Business of Government receives a message with an attachment that looks as though it has come from a co-worker, then the employee is more likely to open it.

Why Social Media are Vulnerable

A social media message can have a file attached to it and this could be infected.

Risk Mitigation Activities

Because many offices use e-mail to send files, it may not be feasible simply to ban the practice. Short of that fail-safe method to counter this threat, there are measures that end users, managers, and IT staff can take to mitigate this risk.

By users

- Watch out for messages which require guesswork by user to determine subject and sender of the e-mail.
- Exercise caution in opening files attached to e-mails and social media messages.

By management

- Make a plan documenting security controls and review this plan at regular intervals.
- Decide on the process for handling security issues raised by the general public.

By IT staff

- Continue with the controls that the government organization already has in place to combat malicious e-mail.
- Connect to the Internet via a Trusted Internet Connection. The U.S. federal government has a Trusted Internet Connection program. These connections offer increased levels of security.
- Take measures to protect the actual PCs used by users.
- Use tools to monitor user behavior so that a check can be made on whether policy is being observed.
- Install the latest web browsers on PCs; they are likely to have better security controls than older browsers.
- Consider storing all communication, if it is technically feasible.
- Make users aware of the risks involved and give them examples of the types of attack.
- Make users aware of the organization's AUP.
- Make users aware of the legal issues.
- Repeat awareness development and training at regular intervals.

SOCIAL MEDIA WEBSITES

Understanding the Risk

With the advent of interactive websites, hackers gained a way to install malware on a user's computer through seemingly innocuous means—sometimes without the user even being aware that their machine was being infected at all. Using any one of a number of technologies—AJAX, Java, and DirectX are examples—and in combination with spoofing or social engineering, hackers can bypass security software and introduce malware.

Why Social Media are Vulnerable

Visitors to social media websites do not always know how vulnerable the website is to security breaches. Although a security standard has recently been developed for web application developers to adhere to, it is difficult to know if a particular website is adhering to it or not. The standard is the Application Security Verification Standard, developed by the Open Web Application Security Project. It specifies four levels of security control provision.

Risk Mitigation Activities

Threats from websites are emerging all the time, and it can be difficult for end users to keep abreast of all the dangerous websites. Even well-known websites can fall victim to hackers—in fact, the most popular websites are also the most tempting targets due to their large audience. Still, end users, managers, and IT staff all can play a part in reducing this risk.

By users

- Use a password that is at least 10 characters long and has a mixture of letters, numbers, and symbols. Use a different password for each website, so that if a cybercriminal discovers one password, the user's identity at only one website is compromised.

- Before creating a password, ask “what personal information is available about me online?” (The new password should not contain any of this information. When setting up a password, a website often asks the user to specify security questions and the answers to them. Do not select questions or answers containing personal information available online.)
- Exercise caution when using third-party applications within social media websites.

By management

- Make a plan that documents the security controls and review this plan at regular intervals.
- Decide on the process for handling security issues raised by the general public.
- Perform a risk assessment. Making use of social media may expose a government organization to new security risks. A risk assessment can analyze these new risks. Consider asking an independent party to give a risk assessment.
- Put all social media products in one of four categories: can be used at work or at home; can only be used at work, i.e., from behind the office firewall; can only be used only on certain office PCs, either those that have better security or those that are isolated from the bulk of the office network; or cannot be used anyplace.
- Consider only social media websites that have a responsible attitude toward security. Consider the purpose given for using social media and look into the specifics of the particular website(s) that have been recommended.
- Make a plan to review the security controls implemented by the social media provider.
- Develop an AUP specifying the rules of behavior when using social media. Among other things, this should inform employees and the general public of what information can and cannot be posted on the social media website.
- The Security Operations Center (SOC) of the government organization needs to interact with the security experts of the social media provider. Make the roles and responsibilities of both parties clear. The SOC should ensure that the social media provider is adhering to government policy.
- Ask the social media website provider to make the government organization aware of proposed configuration changes.

By IT staff

- Continue with the online usage controls that the government organization already has in place to combat rogue websites.
- Connect to the Internet via a Trusted Internet Connection. The U.S. federal government has a Trusted Internet Connection program. These connections offer increased levels of security.
- Take measures to protect the actual user PCs.
- Use tools to monitor user behavior so that a check can be made on whether policy is being adhered to.
- Install the latest web browsers on PCs; they are likely to have better security controls than older browsers.
- Consider storing all communication, if it is technically feasible.
- Decide which websites, or content, users are prohibited from viewing and filter websites accordingly. Many filters on the market have advanced features that can grant different levels of permissions for different users, based on their roles and social media needs.
- Consider using a “sandbox,” a digital virtual environment, to test new social media websites and applications.
- Consider separating the network used for social media access from the one used for general office use, so as to isolate any security breaches should they occur.
- Consider reaching out to the administrators of social media websites frequented by users in your office, and coordinate with them to encourage strong authentication mechanisms.
- If the government has negotiated a security contract with the social media website owners, then the government organization’s SOC should monitor adherence of the website owners to the contract. This includes logging incidents and the speed with which they are addressed.
- Make users aware of the risks involved and give them examples of the types of attack.
- Make users aware of the organization’s AUP.
- Make users aware of the legal issues.
- Train users in the safe usage of social media websites.
- Repeat awareness development and training at regular intervals.

UNSECURED DATA STORAGE DEVICES

Understanding the Risk

Even computers and networks that are not connected to the Internet are in danger of being infected by malware through the unwitting use of portable data storage devices, such as the ubiquitous thumb drives. In the most high-profile case, a worm called Stuxnet was transmitted into a closed computer network when someone used an infected thumb drive on an otherwise secure computer. The result was a severely compromised network.

Why Social Media are Vulnerable

The availability of small portable data storage devices, such as thumb drives, allows data intended for uploading to social media to be introduced behind the government department's firewall. Further, the drives themselves are often used by more than one person, increasing the likelihood of malware infection and exposing all users to the risks engendered by the least careful.

Risk Mitigation Activities

Because of the straightforward nature of the attack, this is as easy to prevent as it is to occur. Through end user behavior or technical activity, data storage devices should simply not be used on computers connected to secured networks.

By users

- Adhere to the AUP.

By management

- Make a plan documenting security controls and review this plan at regular intervals.
- Decide on the process for handling security issues raised by the general public.
- Decide on the mobile devices that will be allowed access to PCs.

By IT staff

- Continue with the controls that the government department already has in place.
- Take measures to protect the actual user PCs, i.e., install and regularly update anti-malware controls on all PCs so as to handle infected devices.
- Use tools to monitor user behavior so that adherence to policy can be monitored.
- Make users aware of risks and provide examples of the types of infection.
- Make users aware of the organization's AUP.
- Make users aware of the legal issues.
- Repeat awareness development and training at regular intervals.

Abdul Waheed, S. & Elis, S. (2011, February 13). *PM: No parallels between Egypt and Malaysia*, New Sunday Times, Malaysia.

Bertot, J.C, Jaeger, P.T., Munson, S., Glaisyer, T. (2010, August 12). *Engaging the Public in Open Government: Social Media Technology and Policy for Government Transparency*. Retrieved from www.tmsp.umd.edu/TMSPreports_files/6.IEEE-Computer-TMSP-Government-Bertot-100817pdf.pdf

Catholic Education Office, Sydney. (2011, February 21). Staff Use of Social Media in Sydney Catholic Schools. Retrieved from www.ceosyd.catholic.edu.au/Parents/Curriculum/Documents/pol-socialmedia-staff.pdf

Chief Information Office. (2009, September). *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*, Version 1.0.

City of Chandler, Arizona. (2009, August). *Administrative Regulation: Social Media/Social Networking*. Retrieved from http://icma.org/en/icma/knowledge_network/documents/kn/Document/300737/Social_Media_Policy__City_of_Chandler_AZ

Coleman, C. (2009, August 25). *Web 2.0 Tools Encourage Public Debate*, Remarks at the CRM Evolution 2009, New York. Retrieved from www.gsa.gov/portal/content/103720

Computers, Freedom, and Privacy Conference. (2008). *Technology Policy '08*. Retrieved from www.cfp2008.org/wiki/index.php/Main_Page

comScore, Inc. (2011, February). *U.S. Digital Year in Review 2010: A Recap of the Year in Digital Media*.

De Jong, J., and Rizvi, G. (eds.) (2009). *The State of Access: Success and Failure of Democracies to Create Equal Opportunities (Innovative Governance in the 21st Century)*. Brookings Institution Press.

REFERENCES

- Drapeau, M. & Wells II, L. (2009, April). *Social Software and National Security: An Initial Net Assessment*, Center for Technology and National Security Policy, National Defense University. Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525
- Edelman, B. (2011, January–February). *Adverse selection in online ‘trust’ certifications and search results*. *Electronic Commerce Research and Applications*, Volume 10, Issue 1, Pages 17–25.
- European Union, Ministers for eGovernment Policy. (2009, November 18). *Ministerial Declaration on eGovernment*. Retrieved from www.egov2009.se/wp-content/uploads/Ministerial-Declaration-on-eGovernment.pdf
- Governor, J., Hinchcliffe, D., Nickull, D. (2009). *Web 2.0 Architectures*, O’Reilly.
- Hrdinova, J., Helbig, N., and Peters, C.S. (2010, May). *Designing Social Media Policy for Government: Eight Essential Elements*, Center for Technology in Government, University of Albany, New York. Retrieved from www.ctg.albany.edu/publications/guides/social_media_policy/social_media_policy.pdf
- Kundra, V. (2009, May 19). *The State of Federal Information Security*. Retrieved from www.cio.gov/pages.cfm/page/Vivek-Kundra-Testimony-on-the-state-of-Federal-information-security
- Lavasoft AB. (2010, June). 9 Ways to Control Your Privacy on Social Network Sites. Retrieved from www.lavasoft.com/company/newsletter/2010/06/article_9_ways_to_control_your_privacy_on_social_networking_sites.php
- Lazer, D., Neblo, M., Esterling, K., Goldschmidt, K. (2009) *Online Town Hall Meeting: Exploratory Democracy in the 21st Century*, 2009 Congressional Management Foundation, Washington, D.C. Retrieved from www.cmfweb.org/storage/cmfweb/documents/CMF_Pubs/online-town-hall-meetings.pdf
- Lim, P. (2011, April 29). *Singapore’s top satirist thrives in election season*, AFP News. Retrieved from <http://sg.news.yahoo.com/singapores-top-satirist-thrives-election-season-025109933.html>

- O'Reilly, T. (2005, September 30). *What is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software*. Retrieved from <http://oreilly.com/web2/archive/what-is-web-20.html>
- Obama, B. (2009, January). Memo on *Transparency and Open Government*. Retrieved from <http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf>
- Pelgrin, W.F. (2010, March). *Security and Privacy on Social Networking Sites*, Monthly Security Tips – Newsletter, Vol. 5, Issue 3, MS-ISAC. Retrieved from <http://msisac.cisecurity.org/newsletters/documents/2010-03.pdf>
- Province of British Columbia, Office of the Chief Information Officer. (2010). *Use of Social Media in the B.C. Public Service*, Version 3. Retrieved from www.cio.gov.bc.ca/local/cio/informationsecurity/policy/summaries/33_social_media.pdf
- Rico, S., Bradley, B., Kiefer, M. (2010). *USA Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, ISACA, Rolling Meadows, IL 60008, USA.
- Scherer, M. (2011, May 30). *Can They Win, One Tweet at a Time?*, Time.
- State of California, Office of the State Chief Information Officer. (2010, February). *Social Media Standard SIMM 66B*. Retrieved from www.cio.ca.gov/Government/IT_Policy/pdf/simm_66b.pdf
- Thomas, K., Grier, C., Nicol, D.M. (2010). *unFriendly: Multi-party Privacy Risks in Social Networks*, in *Privacy Enhancing Technologies*, eds. Atallah, M.J., Hopper, N.J., Lecture Notes in Computer Science, Springer Berlin / Heidelberg.
- Viet Nam News. (2011, April 29). Retrieved from <http://vietnamnews.vnagency.com.vn/Social-Issues/210853/Anti-govt-propagandist-arrested.html>

Dr. Alan Oxley is a Professor in the Computer and Information Sciences Department (CIS) at Universiti Teknologi PETRONAS. CIS has several staff and graduate students undertaking research in e-government. At the university, Dr. Oxley supervises a number of graduate students, two of whom are conducting research on Web 2.0—one on mash-ups and one on social networking. Oxley is a chartered member of the British Computer Society. He has been an active member, writing a number of articles for the society's publications.

Dr. Oxley received his Ph.D. in Engineering (thesis title: "Computer Assisted Learning of Structural Analysis") from Lancaster University, United Kingdom. He teaches courses on software agents and software architecture and patterns. He recently revamped the software architecture course to make it more relevant to Web 2.0. Dr. Oxley produced the acceptable use policy for the previous university at which he was employed; see the article published in *Educause Quarterly 2005*, "Formulating a Policy on IT Provision." He has obtained grant funds for computer science research.

Dr. Oxley has a number of research interests, a key one of which is IT service management. He has written articles and conducted presentations on a variety of topics. Dr. Oxley is currently at work preparing for his role in a 2012 conference.

Acknowledgment

The author wishes to thank Rabiul Ibrahim, a graduate research assistant from the Computer and Information Sciences Department at Universiti Teknologi PETRONAS, for his contributions to this report.

To contact the author:

Dr. Alan Oxley, MBCS, CITP, CEng

Professor

Computer and Information Sciences Department

Universiti Teknologi PETRONAS (UTP)

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

Malaysia

605-368 7517

e-mail: alanoxley@petronas.com.my

UTP website: www.utp.edu.my/

Oxley's website: www.utp.edu.my/staff/ex.php?mod=ex&sn=132723



REPORTS from
The IBM Center for The Business of Government

Assessing the Recovery Act

Managing Recovery: An Insider's View by G. Edward DeSeve

Virginia's Implementation of the American Recovery and Reinvestment Act: Forging a New Intergovernmental Partnership by Anne Khademian and Sang Choi

Collaborating Across Boundaries

Environmental Collaboration: Lessons Learned About Cross-Boundary Collaborations by Kathryn Bryk Friedman and Kathryn A. Foster

Managing Innovation Prizes in Government by Luciano Kay

Conserving Energy and the Environment

Implementing Sustainability in Federal Agencies: An Early Assessment of President Obama's Executive Order 13514 by Daniel J. Fiorino

Breaking New Ground: Promoting Environmental and Energy Programs in Local Government by James H. Svara, Anna Read, and Evelina Moulder

Fostering Transparency and Democracy

Assessing Public Participation in an Open Government Era: A Review of Federal Agency Plans by Carolyn J. Lukensmeyer, Joe Goldman, and David Stern

Using Geographic Information Systems to Increase Citizen Engagement by Sukumar Ganapati



REPORTS from
The IBM Center for The Business of Government

Improving Performance

A Leader's Guide to Transformation: Developing a Playbook for Successful Change Initiatives by Robert A. F. Reisner

A Guide to Data-Driven Performance Reviews by Harry Hatry and Elizabeth Davies

Project Management in Government: An Introduction to Earned Value Management (EVM) by Young Hoon Kwak and Frank T. Anbari

Managing Finances

Strategies to Cut Costs and Improve Performance by Charles L. Prow, Debra Cammer Hines, and Daniel B. Prieto

Strengthening Cybersecurity

A Best Practices Guide to Information Security by Clay Posey, Tom L. Roberts, and James F. Courtney

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers by Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams

Transforming the Workforce

Engaging a Multi-Generational Workforce: Practical Advice for Government Managers by Susan Hannam and Bonni Yordi

Implementing Telework: Lessons Learned from Four Federal Agencies by Scott P. Overmyer

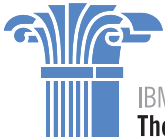
Using Technology

Reverse Auctioning: Saving Money and Increasing Transparency by David C. Wyld

Using Online Tools to Engage—and be Engaged by—The Public by Matt Leighninger

An Open Government Implementation Model: Moving to Increased Public Engagement by Gwanhoo Lee and Young Hoon Kwak

How Federal Agencies Can Effectively Manage Records Created Using New Social Media Tools by Patricia C. Franks



IBM Center for
The Business of Government

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit: ibm.com

For more information:

Jonathan D. Breul

Executive Director

IBM Center for The Business of Government

600 14th Street NW

Second Floor

Washington, DC 20005

202-551-9342

website: www.businessofgovernment.org

e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:



or, send us your name and e-mail to receive our newsletters.