o

SET: Social Networking Sites

Ad

Security for Emerging Technology: Social Networking Sites

(U) This training steps you through the emerging risks posed by evolving technologies as it applies to social networking sites. Learn best practices for maintaining security, preventing security incidents, and recovering from a security incident.

(U) By the end of this training, you will be able to:

- Define the term, social networking site
- Identify the risk
- Identify the security best practices
- Identify appropriate incident responses

WHO SHOULD ATTEND: Recommended for anyone who uses social networking sites, or has family or friends that use social networking sites.

REGISTRATION:

REFERENCE MATERIALS:

NONE

COURSE DETAILS:

- **(U) Overall Course Classification:** UNCLASSIFIED//FOR OFFICIAL USE ONLY
- **(U) Delivery Method:** Web-based Training
- **(U) Duration:** 10 minutes
- **(U) Minimum System Requirements:** Internet Explorer 7 and Flash Player 10+

DELIVERY: Computer Based / Web-Based

COURSE LENGTH: 0

CLASSIFICATION: UNCLASSIFIED

ONLINE TRAINING

Launch Training

NROU SCHOOL

School of Security

SPONSOR

Office of Security and Counterintelligence

COURSE PROVIDER

Office of Security and Counterintelligence

(b)(3)

View Guidelines

Security for Emerging Technology | Social Networking Sites

Introduction

(U) Security for Emerging Technology | Social Networking Sites

Title page

(U) Welcome to **Social Networking Sites**, part of our **Security for Emerging Technology** curriculum.

Intro page

(U) Join us on a walk-through of the emerging risks posed by evolving technologies. Learn best practices for maintaining security, preventing security incidents and recovering from a security incident.

(U) Objectives

(U) By the end of this topic, you will be able to:

- Define the term
- Identify the risk
- Identify security best practices
- Identify appropriate incident responses

Button: Test Yourself!
Get 80% and you're done!

(U) We recommend you take the pre-test before beginning the topic. If you can answer 80% of the questions correctly, you will receive credit for this topic.

Button: Start the Topic!
Learn how you can be secure!

Body

(U) Vignette

(U) Disclaimer: The Onion News Network is not a real news network. It is a satire site.

(U) What Are They?

(U) Social Networking Sites are designed to encourage making connections and sharing information.

(U)Any Online service, platform or site that allows users to post information on a personal profile and network with others via a list of contacts can be considered a Social Networking Site. They include blogs, microblogs, photo and video sharing sites, collaborative wiki's and more.

(U) What is the Risk?
(U) Careless participation could:

- Reveal sensitive information
- Compromise sensitive operations

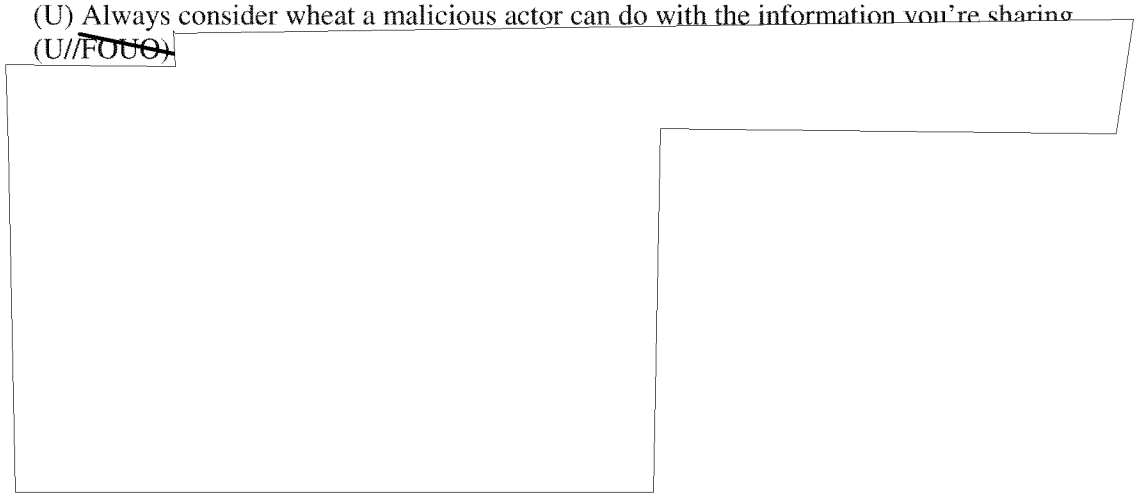
- Set up self or others for further targeting
- Infect system with malware
- Enable identity theft

(U) Examples

(U) Click an example from the list on the left to view additional information.

(U) OPSEC Violation (Facebook)

(U) Always consider wheat a malicious actor can do with the information you're sharing (U//~~FOUO~~)



(U) How useful would his photos be to someone planning an attack?

(U) OPSEC Violation (Facebook)

(U) Not only do you need to practice OPSEC, you need to watch your network.

(U//~~FOUO~~) In December 2011, an F-15E squadron out of Europe received orders for a short-notice, out-of-cycle deployment to Afghanistan. All December leave was cancelled to prepare for deployment.

(U) An adversary, following the social network connections, can now learn the deployment details.

(U) Spear-Phishing (LinkedIn)

(U) Like email, you must be alert when using Social Networking Sites for phishing, malware and other online scams.

(U) Spear-phishing is a kind of social engineering trick aimed at a specific victim.

(U) A spear-phishing message might include not only your name but other specific information (mentions of friends by name, organizational references) that helps personalize it and make it believable. Spear-phishers can draw this information from social networks.

(U) Phishing (Facebook)

(U) This post went up mere hours after the death of Apple co-founder Steve Jobs.

(U) In six hours, over 15,000 users had clicked the link and been sent to websites to fill out surveys or sign up for free offers.

(U) Every click generated paid affiliate fees for the scammers.

Graphic: logos

(b)(3)

Graphic: FOB pic

Graphic: network

Graphic: phishing email

(U) Privacy Loophole (Skype)

(U) Use your privacy and security settings, but don't rely on them – even the most restrictive privacy controls can't protect against loopholes or security flaws in the service.

(U) Researchers found a vulnerability in Skype, a popular service for video chat over the internet, which can expose your location, identity, and the content you're downloading.

(U) Skype tracks user's location over time and any peer-to-peer file sharing activity. A caller using a VoIP (Voice over IP) system can ibtain the recipient's IP address when establishing the call. They can then user commercial geo-IP mapping services to determine the other user's location and Internet Service Provider (ISP).

(U) They also found it was possible to obtain the user's IP address without alerting them to the call attempt, without being on their contact list, and even if the user had explicitly configured Skype to block calls from non-contacts.

Graphic: RIP Steve Jobs

Graphic: bitly count

(U) Identity Theft (Mock Site)

(U) What information is risky? Mouse-over areas to view the danger.

(U) What Can I Do?

(U) Know your exposure – different sites are designed to share information in different ways.

- Know where your information is
- Know who and what can access it

(U) Monitor your online identity.

- Just because you aren't posting, doesn't mean other aren't posting about you.

(U) When browsing:

- Be wary of links and online scams.

(U) Always logout and close the browser window when finished.

- Social Networking Sites can collect information on you when you visit other sites while logged in to their site.
- Closing only the page tab will not log you out; you must close the window.

Graphic: mock site (with rollovers)

(U) What Can I Do?

(U) When creating a profile:

- Limit personal or identifying information on your profile. Most fields are not required.
- Use unique password and change it regularly. A password manager can help manage accounts – or you can write them down.
- Set your privacy settings and review them regularly. When a site updates or changes features, it can reset your settings to the default, which is usually "public or "opt-out".
- Don't friend anyone you don't know.
    - Verify identity through outside channels. Just as you can enter false information in your profile, so can other people.

(U) Applications:

- Restrict which applications can access your profile and what data they can access. Don't hesitate to refuse an application if it wants more access than you're comfortable with.

(U) What Can I Do?

(U) Before posting ask yourself:

- Why are you sharing this?
- Who will be able to see it?
- What metadata will be associated with it?

- What will people do with the information?
- What can be learned from it if aggregated with other information?
- How will this information be transmitted and stored?
- How can I delete it if I change my mind?

(U) When posting:

- Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family and friends.
- Use filters to restrict who can see your posts.
- Even with filters, never put anything online you wouldn't feel comfortable with the whole Internet seeing.
- Never provide passwords, credit card information, or money to someone via SNS.

(U) No One's Perfect

(U) If you see something posted to a Social Networking Site that you believe violates OPSEC:

- Do NOT comment on the site.
- Report it to your cognizant Security Officer.

(U) If you need to delete information or a post:

- Delete it immediately.
- If the information was classified, report it to your cognizant Security Officer.

(U) Question 1

(U) Question 2

(U) Question 3

(U) Question 4

(U) Question 5

Graphic: failbook

Rollover: **Error! Not a valid bookmark self-reference.**

Rollover: Personal information

Graphic: Photos of credit cards

Graphic: posted pii

Conclusion

(U) Congratulations!

(U) You have completed the SET: Social Networking Sites lesson. You may print your certificate or exit the course now.

Questions

(U) Pretest

(U) Directions: Evaluate the following statements about Social Networking Sites as TRUE for FALSE. Click done to submit your answer.

(U) Social Networking Sites encourage building social networks and haring information.
- A. True **
- B. False

(U) You must fill in all profile information when creating an account.
- A. True
- B. False **

(U) Profile information is always true.
- A. True
- B. False**

(U) Most Social Networking Sites are "opt-in" as their default.
- A. True
- B. False **

(U) Once set, security and privacy settings never need to be revisited.
- A. True
- B. False **

(U) It's ok to post anything that's UNCLASSIFIED.
- A. Ture
- B. False **

(U) You should not have an expectation of privacy when using a Social Networking Site.
- A. True **
- B. False

(U) Deleting a post, or your account, removes that information from everywhere it's stored.
- A. True
- B. False **

(U) You do not need to worry about phishing, malware, or other scans on Social Networking Sites.
- A. Ture
- B. False **

(U) Sharing personally identifiable information can lead to identity theft.
- A. True **
- B. False

(U) Social Networking Sites can collect information on you when you visit other sites while logged in to their site.
- A. Ture **
- B. False

(U) Programs can be opt-in or opt-out.
- Opt-in: you are not enrolled but have the option to join in.
- Opt-out: you are automatically enrolled and have the option to be taken out.

(U) Question #1

(U) You must fill in all profile information when creating an account.
A. True
B. False **

(U) Profile information is always true.
A. True
B. False **

(U) Question #2

(U) Most Social Networking Sites are "opt-in" as their default.
A. True
B. False **

(U) Once set, security and privacy settings never need to be revisited.
A. True
B. False **

(U) Question #3

(U) It's ok to post anything that's UNCLASSIFIED.
A. Ture
B. False **
(U) You should not have an expectation of privacy when using a Social Networking Site.
A. True **
B. False
(U) Deleting a post, or your account, removes that information from everywhere it's stored.
A. True
B. False **

(U) Question #4

(U) You do not need to worry about phishing, malware, or other scans on Social Networking Sites.
A. Ture
B. False **
(U) Sharing personally identifiable information can lead to identity theft.
A. True **
B. False

(U) Question #5

(U) Social Networking Sites can collect information on you when you visit other sites while logged in to their site.
A. Ture **
B. False

Graphics and Additional Information

Rollover Textbox: **Error! Not a valid bookmark self-reference.**
Metadata for a post can include:

- Time

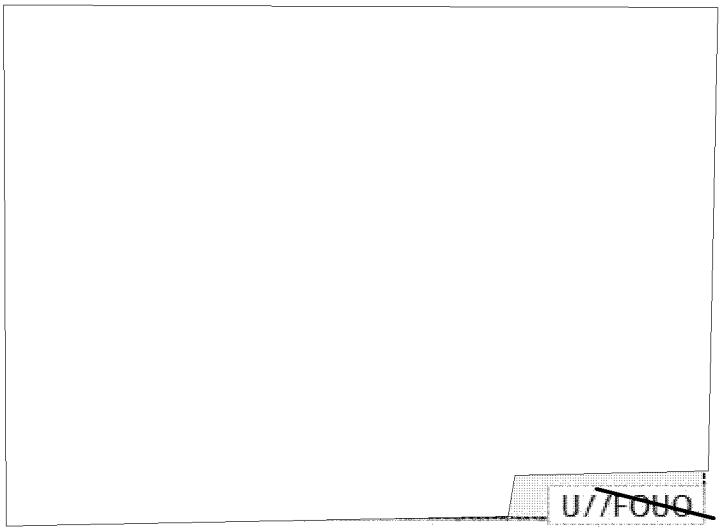
- Location
- Method (web, mobile, app, etc.)
- IP address

Rollover Textbox: personal information
In addition to Personally Identifiable Information, this includes personal health information:

- Prescriptions
- Allergies
- Medical conditions
- Primary care physician mane and location

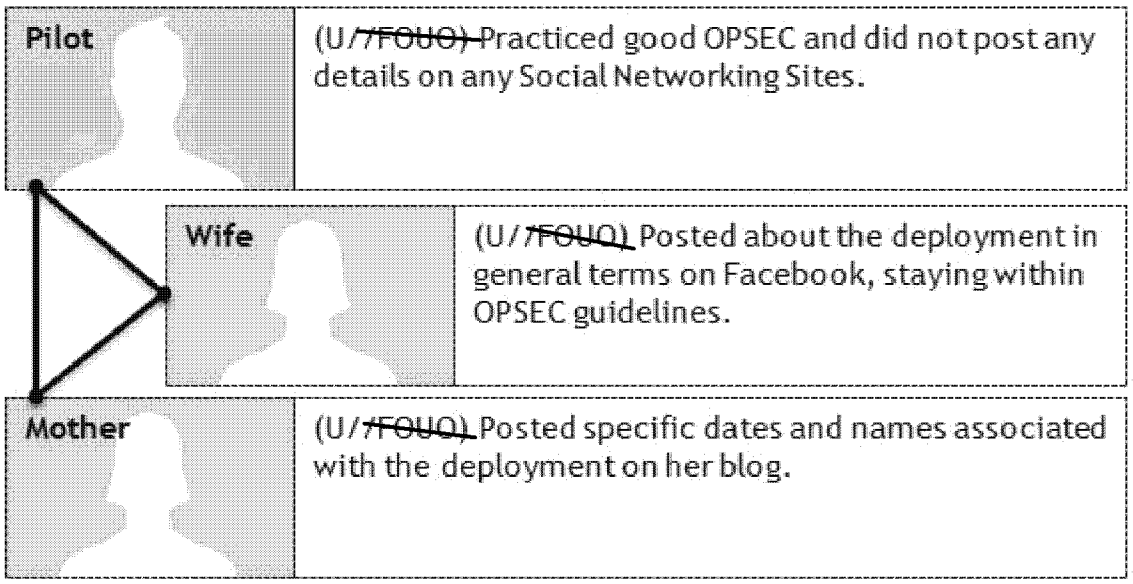
Graphic: logos

Graphic: FOB pic



(b)(3)

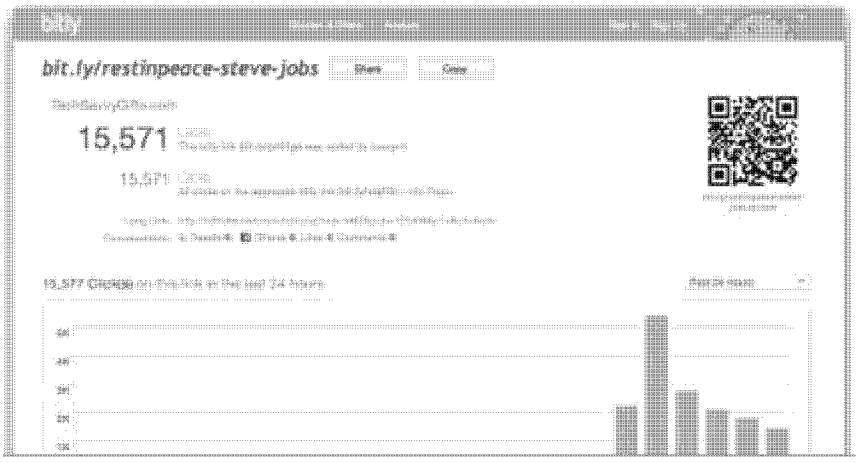
Graphic: Network



Graphic: phishing email

Graphic: RIP Steve Jobs

Graphic: bitly count

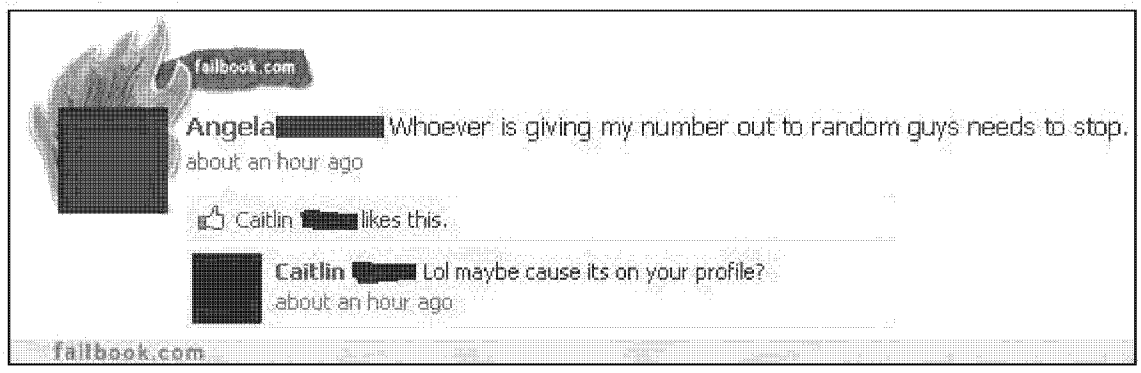


Graphic: Mock site

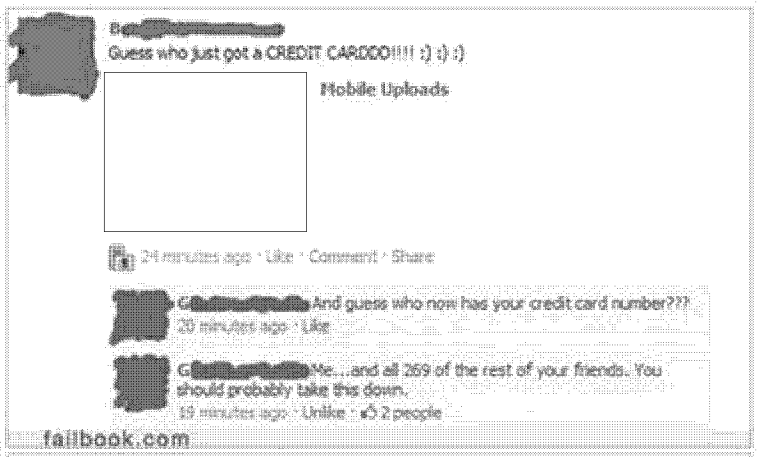
(b)(3)

Rollovers
(U) Provides your full name.
(U) Head shot can be used to create a fake id.
(U) Tells people you will be out of town.
(U) Identifies your bank.
(U) Provides your full name.
(U) Combined with knowledge of when you'll be out of town, identity thieves can steal mail- including credit card applications.
(U) Date of birth is often used on forms and to confirm identity.
(U) This is often your hometown, a key piece of identity data.
(U) People commonly have personal security questions for passwords associated with their pets.
(U) Mother's maiden name is a common security verification question.
(U) The game designer may have created the game simply to get registration information.

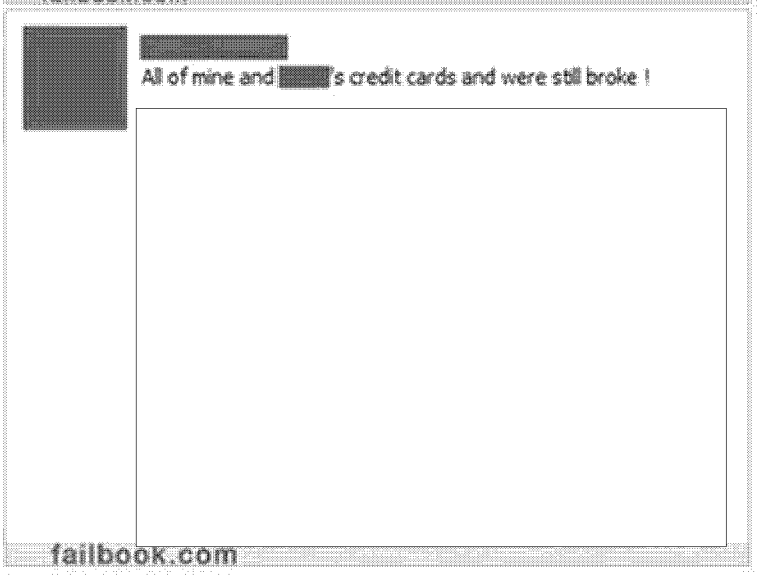
Graphic: failbook



Graphic: photos of credit cards



(b)(3)



(b)(3)

Graphic: posted PII