# Session # 52

## Social Media: Manage the Security to Manage Your Experience

**Ross C. Hughes, U.S. Department of Education**

START HERE
GO FURTHER
FEDERAL STUDENT AID

Information Systems Security Awareness - Windows Internet Explorer

http://iase.disa.mil/eta/issv4/issv4/module.htm

(1 item remaining) Waiting for http://iase.disa.mil/eta/issv4/issv4/module.ht

Internet | Protected Mode: On

100%

# What’s Out There

START HERE
GO FURTHER
FEDERAL STUDENT AID

# Social Media – Key Features

- Social Networking and Web 2.0
- Member of an online community
- Key features are “Profiles” and “Friend lists”
- The most commonly used is still Facebook
- 2009 saw the rapid emergence of Twitter
- A lot of “Trust” going on
- It is a marketer’s dream

# Let’s Crunch Some Numbers

START HERE
GO FURTHER
FEDERAL STUDENT AID

# Welcome to the Perfect Storm

- In 2009, Facebook announced they had surpassed 300M users. Twitter claims 100M registered users
- Almost 68% of all Internet traffic is social media or search
- Facebook is the 4th largest website in the world having grown 157% between 2008 and 2009 – 1,928% in the US alone
- Social media marketing will grow from $714M in 2009 to $3.1B by 2014*
- Attacks on social media sites is up **240%** from phishing attacks alone
- 

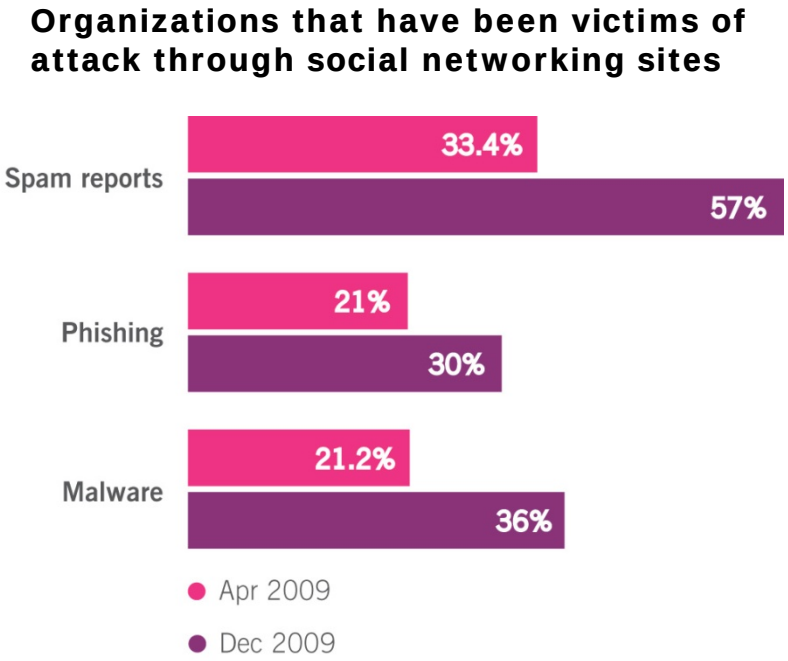
*Forrester Research

START HERE GO FURTHER FEDERAL STUDENT AID

# Attacks Are On The Rise

Spam, phishing and malware attacks through social media are growing:

- 70% rise in firms encountering spam and malware attacks via social networks in 2009
  - Over 50% received spam via social networks
  - Over 33% received malware via social networks




Source: Sophos survey 2010

# And They Are Getting Worse

- **Computer worm -** a self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention

  - **Blaster** (Aug 2003): Infected 55,000 users in the first 24 hours
  - **Code Red** (Jul 2001): Infected 359,000 users in the first 24 hours
  - **Samy** (Oct 2005): Infected **1,000,000** MySpace users in the first 24 hours

# What Else is Out There

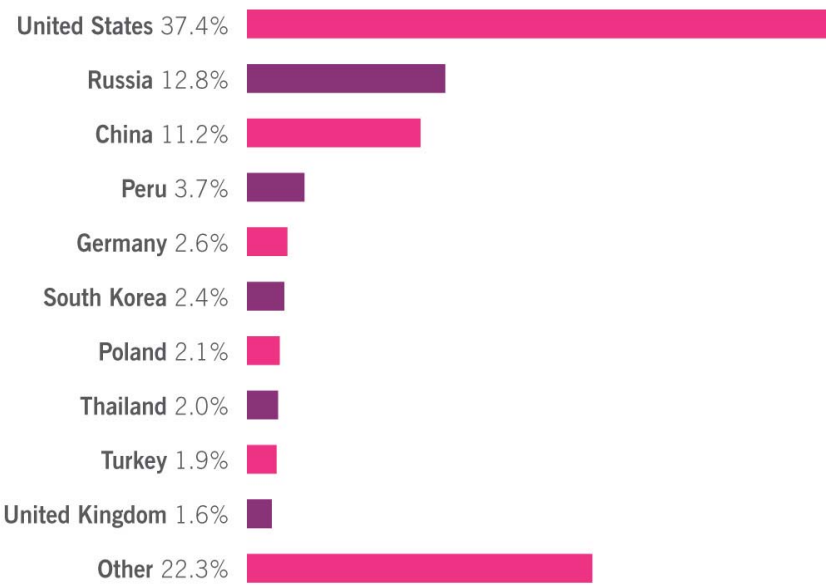
- Almost three quarters of Twitter's 100M accounts are unused or responsible for delivering malicious links
- Easy to use hacker program (Firesheep) that steals Facebook information
- A glitch allows mobile Facebook users to log into other users' accounts
- Twitter worm that posts obscene messages to victims' Twitter feeds
- A Twitter flaw allows messages to pop-up and websites to open in your browser just by moving your mouse over a link

# Being Number 1 – Not So Good

- Over 50,000 web pages hosting malware are discovered EVERY DAY

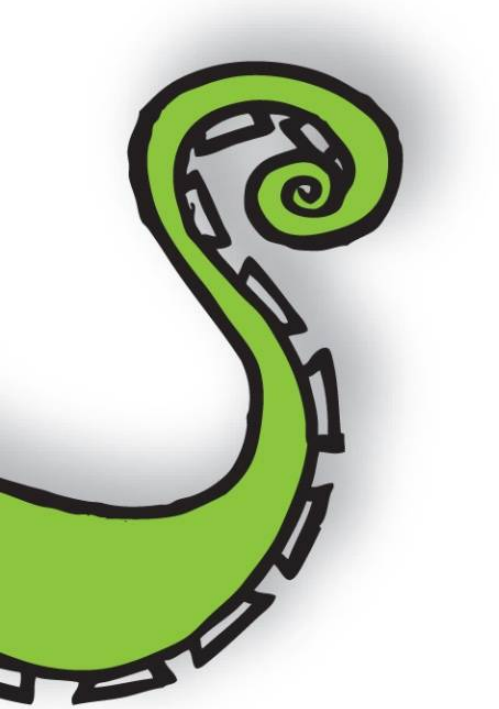
- It's a global problem, with the US at the top of the list for the number of infected web pages

**Top 10 countries hosting malware on the web**




START HERE GO FURTHER FEDERAL STUDENT AID

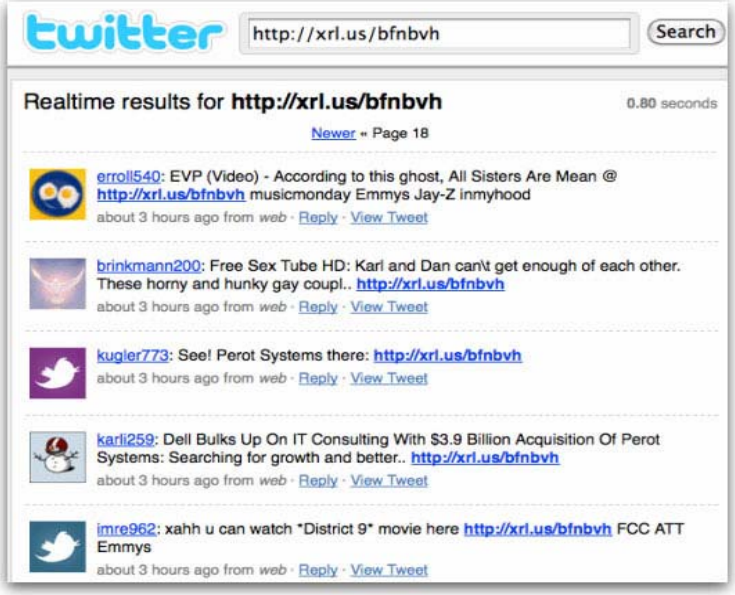
# A Look at the Real World



START HERE GO FURTHER FEDERAL STUDENT AID

# Scareware Tweets

- Scareware is fake anti-virus – instead of protecting your computer it infects it
- Scammers create multiple tweets that direct you to a scareware page. They then try to frighten you into believing you have a security problem and need their software to address it
- Other scareware attacks aim to:
  - Take control of your computer to send spam
  - Hold your computer to ransom
- Result: Malware infection




START HERE GO FURTHER FEDERAL STUDENT AID

# Facebook Privacy Flub

- July 2009: The wife of the chief of the British secret service MI6 posted highly revealing details on her Facebook page
- Her privacy settings meant anyone in the "London" network could view her updates – up to 200 million people
- Information revealed included
  - Family details
  - Personal photos
  - Location of their home
- Result: National security risk

SIS
SECRET INTELLIGENCE SERVICE

START HERE GO FURTHER FEDERAL STUDENT AID

# Fake Tweet to Malware

- A Tweet was posted by Guy Kawasaki, an Apple Mac evangelist with 140,000 followers

  *Leighton Meester sex tape video free download!*

- Following the link hops you to websites offering to show you a video of the Gossip Girl star, but doesn't
- The websites can tell if you are using a Mac or PC … and serves up appropriate malware
- Result: Malware infection

START HERE GO FURTHER FEDERAL STUDENT AID

# Fake Link to Malware

- WHAT.pif botnet
- Malicious Links on popular Facebook pages
- Infected 257,000 accounts
- Could have been worst – Justin Timberlake has 2.1M friends
- Result: Malware infection

START HERE GO FURTHER FEDERAL STUDENT AID

# Fake Facebook Steals the Goods

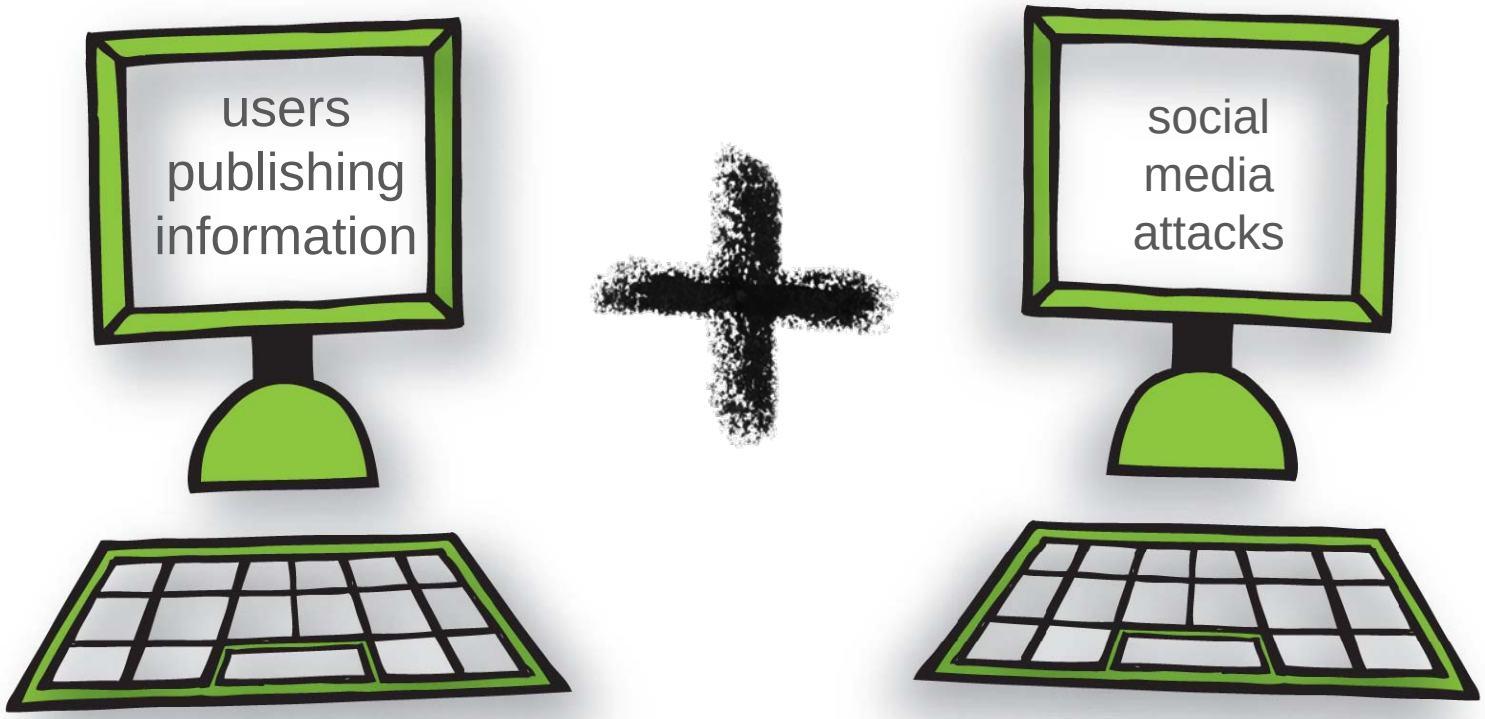
- Ronald Noble, Interpol's Secretary General, has revealed that cybercriminals have opened two fake Facebook accounts using his name and used them to gather sensitive information
  - Obtain information on fugitives targeted during the recent Operation Infra Red
  - Bringing investigators from 29 member countries to exchange information on international fugitives that would lead to more than 130 arrests in 32 countries

# You Just Lost Control

- Here's a message seen spreading across Facebook
- Clicking on the link takes you to what poses as a Fox News TV report
- Once it has your permission, a rogue application will be able send you emails, access your friend lists, gather your personal information, and post messages to your wall
- Result: Compromised account

START HERE GO FURTHER FEDERAL STUDENT AID

# Information Risks

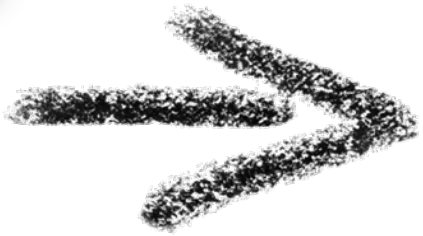



START HERE
GO FURTHER
FEDERAL STUDENT AID

# Users Publishing Information

- Reveal sensitive information
- Defamation of others / organizations
- This can be inadvertent or deliberate
- And the repercussions include
  - Reputation damage
  - Damage to organization
  - Fines

# Motivations Are Changing



Hackers and Script Kiddies
Hobbies/showing off

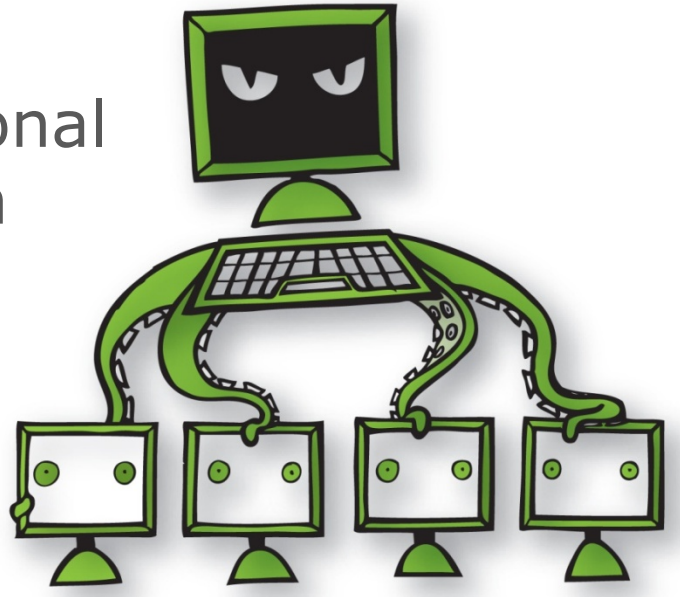
Financially-motivated
organized crime

START HERE
GO FURTHER
FEDERAL STUDENT AID

# Social Media Attacks

- Social media accounts are valuable to hackers
- They can use them to send spam, spread malware, steal identities...

… in the quest to acquire personal information for financial gain



START HERE GO FURTHER FEDERAL STUDENT AID

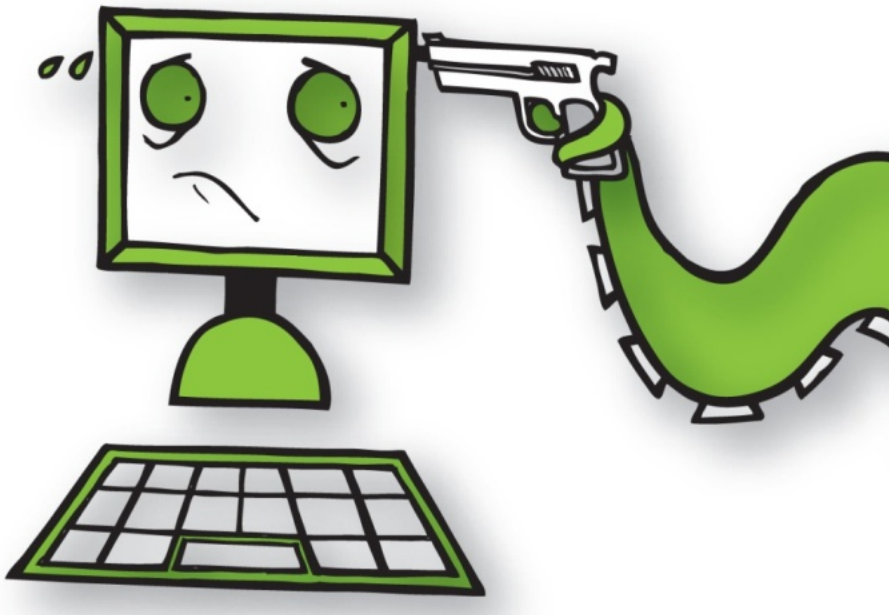
# Data = $$$

- Steal your money directly
- Sell your data
- Trick your friends and family into supplying personal data
- Sell your identity
- Use your accounts to spread spam, malware and more data theft scams
- Sell your organization's data or sensitive information
- Blackmail individuals and organizations

START HERE GO FURTHER FEDERAL STUDENT AID

# How the Threats Work

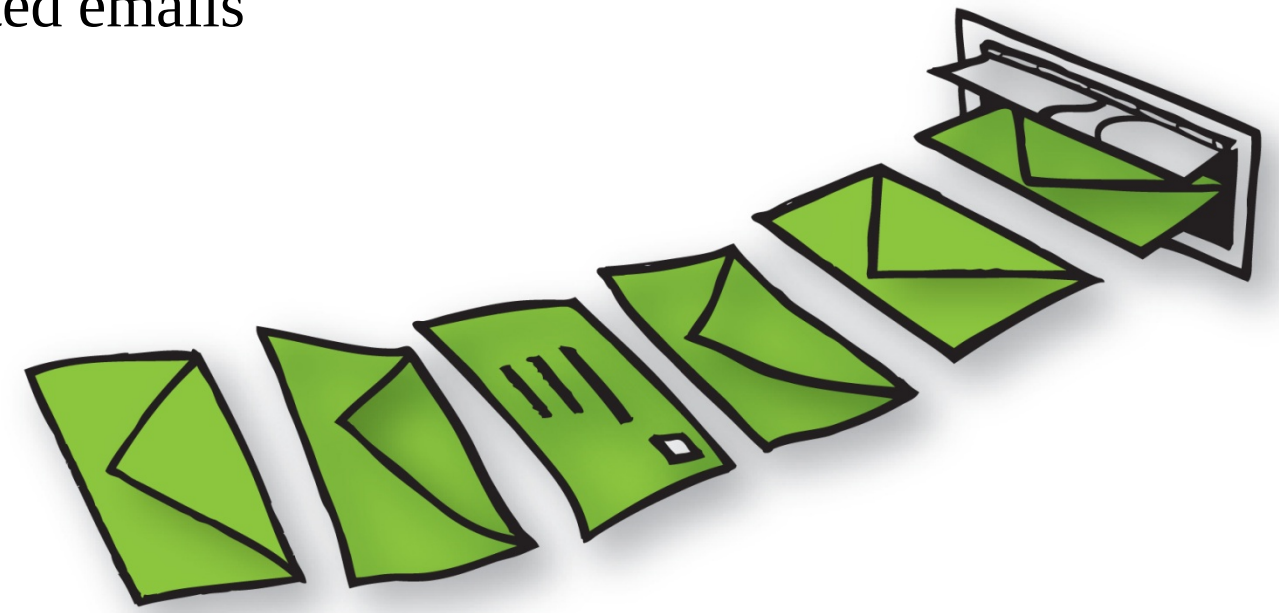
- Spam
- Phishing
- Malware



START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Spam

Unsolicited emails



# Social Media Spam

Click on the link
and you don't get
your Victoria Secret Card

But you do get to visit
this guy

START HERE
GO FURTHER
FEDERAL STUDENT AID

# Social Media Spam

Instead of a job with Google, you may get conned out of $$

START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Spam

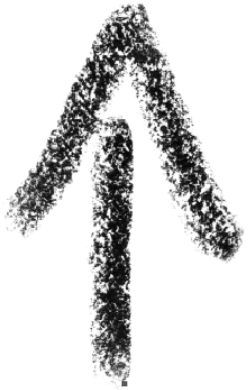
Compromised Facebook account. Victim is now promoting a shady pharmaceutical

START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Spam

57%

of social media users report being hit by spam via these services



That's an increase of

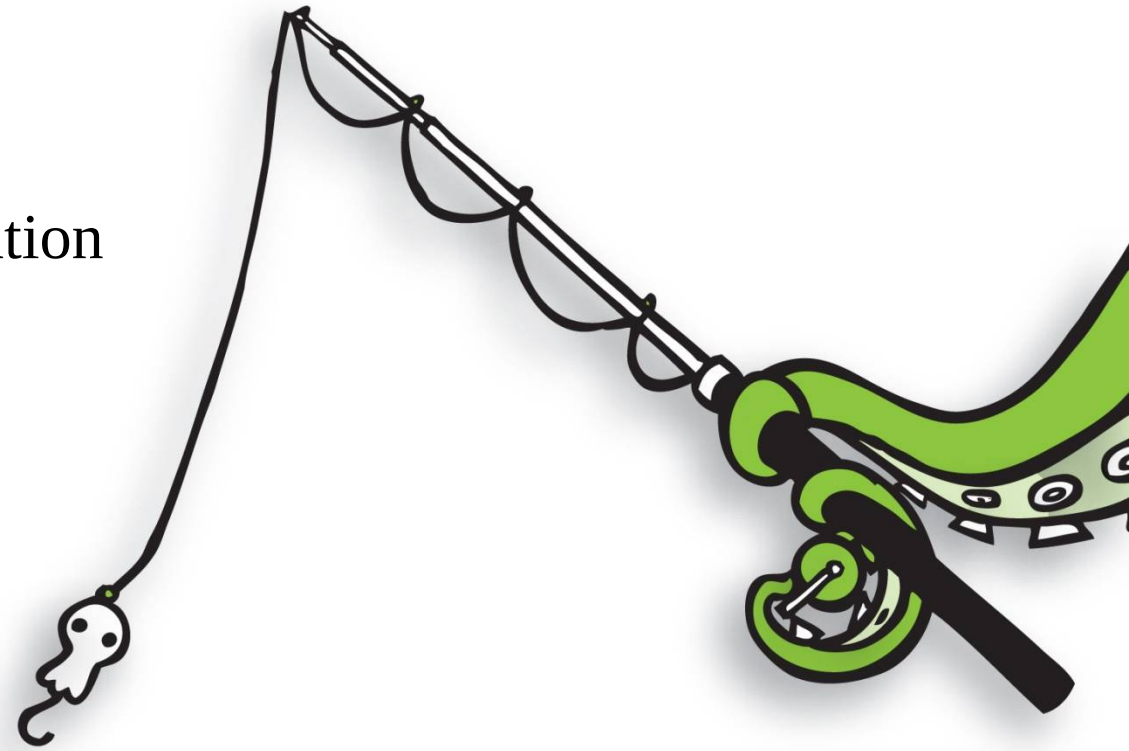
70.6%

from a year ago

START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Phishing

Trying to trick people into revealing sensitive information

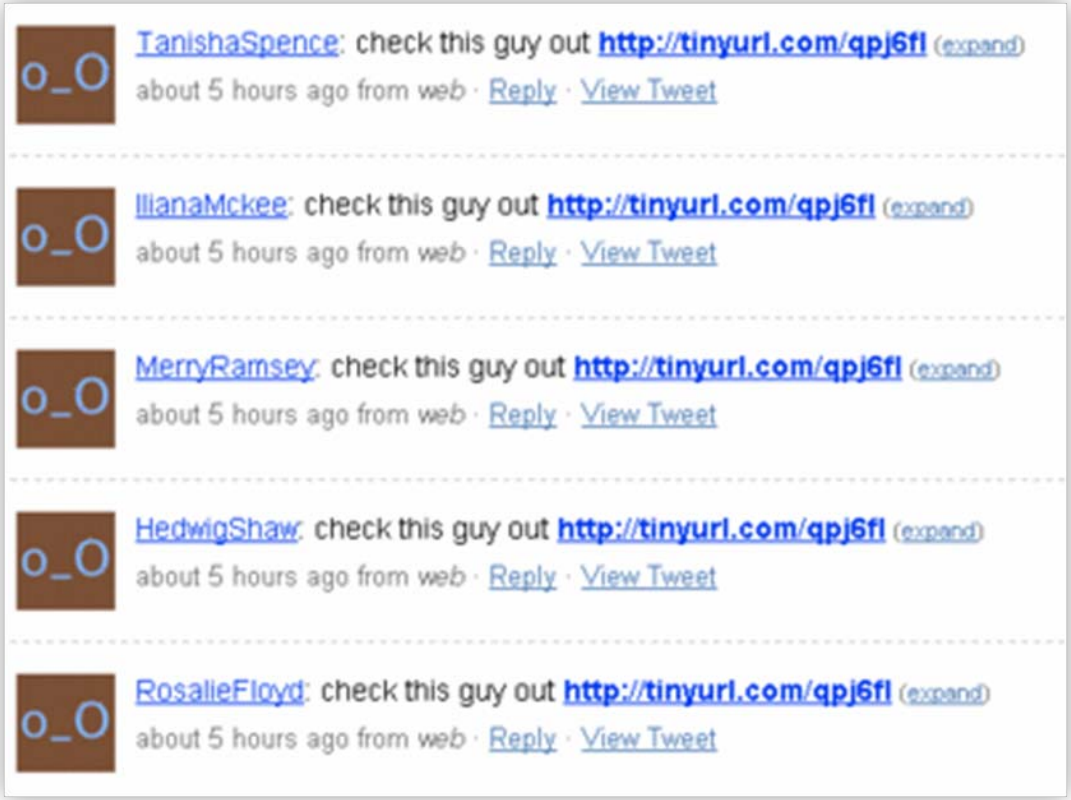


START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Phishing

Trawling the web, trying to hook unwitting victims

Click the link and where do you go?

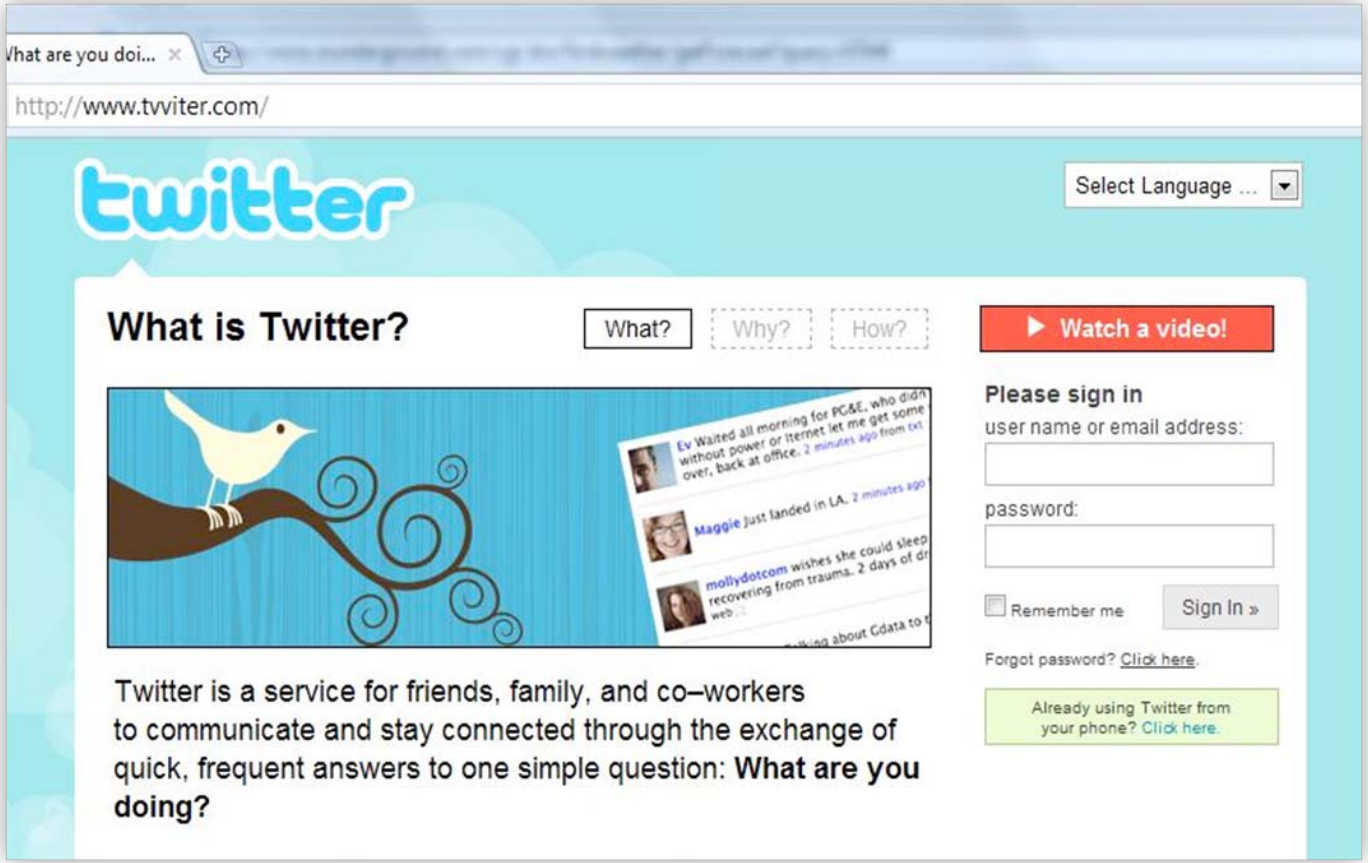



START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Phishing

**To: T V V I T T E R.com**

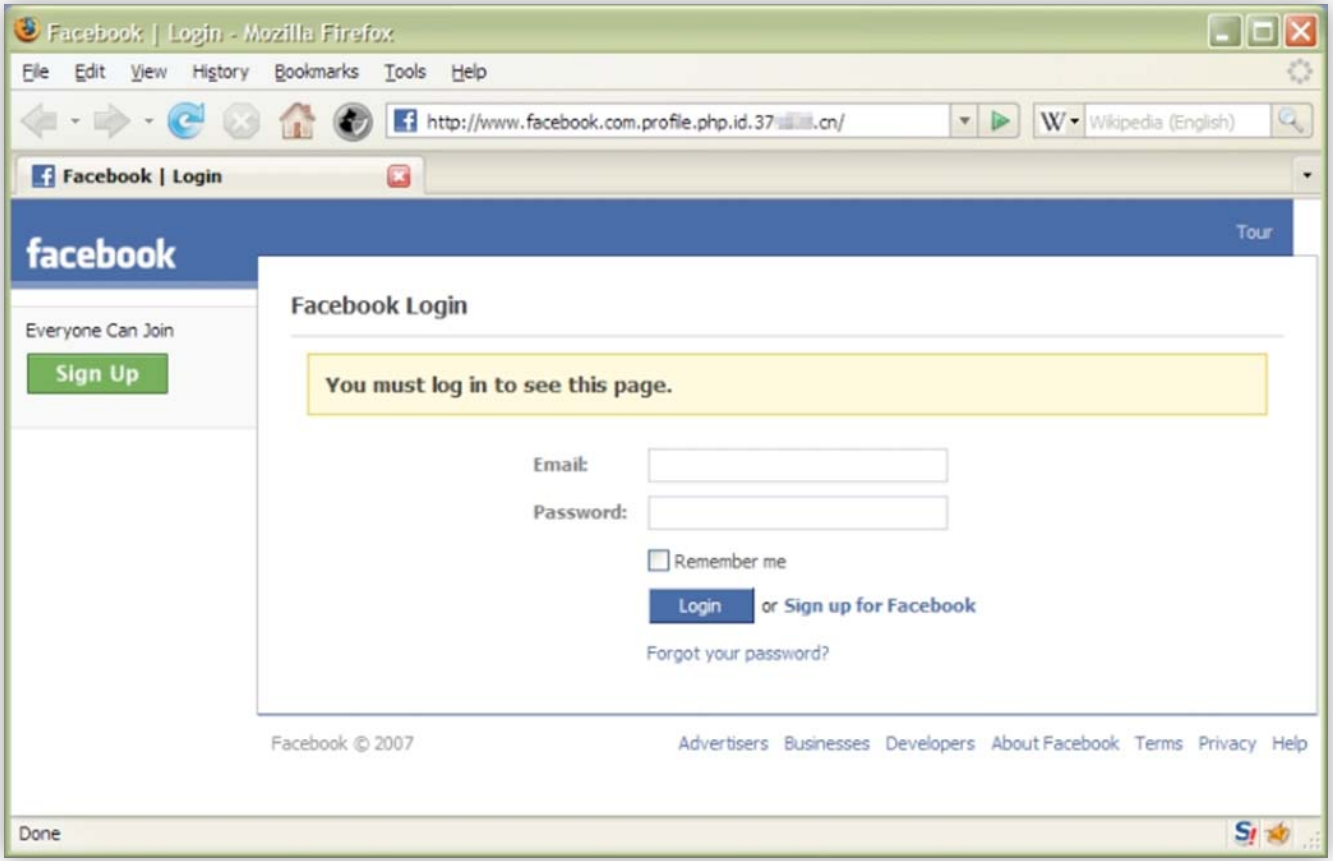
Now they will have your username and password




START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Phishing

Another fake site




START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Phishing

You followed the link, but no immediate fun follows. Instead, you first had to follow what has become a usual procedure for this kind of scam: "like" the page, share the link, complete a survey.

You just earned some money for the scammers, since they are paid for every filled out questionnaire. You have also practically recommended it to your friends, some of which will go on to perpetuate the scam circle.

START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Phishing

30%

of social media users report phishing attacks via these sites

That's an increase of

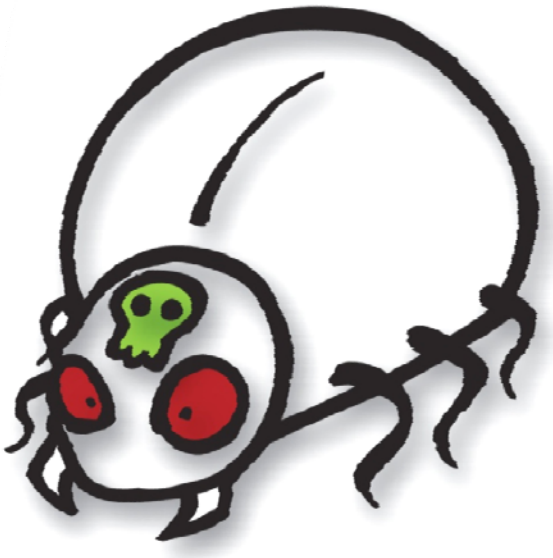
42.9%

from a year ago

START HERE GO FURTHER FEDERAL STUDENT AID

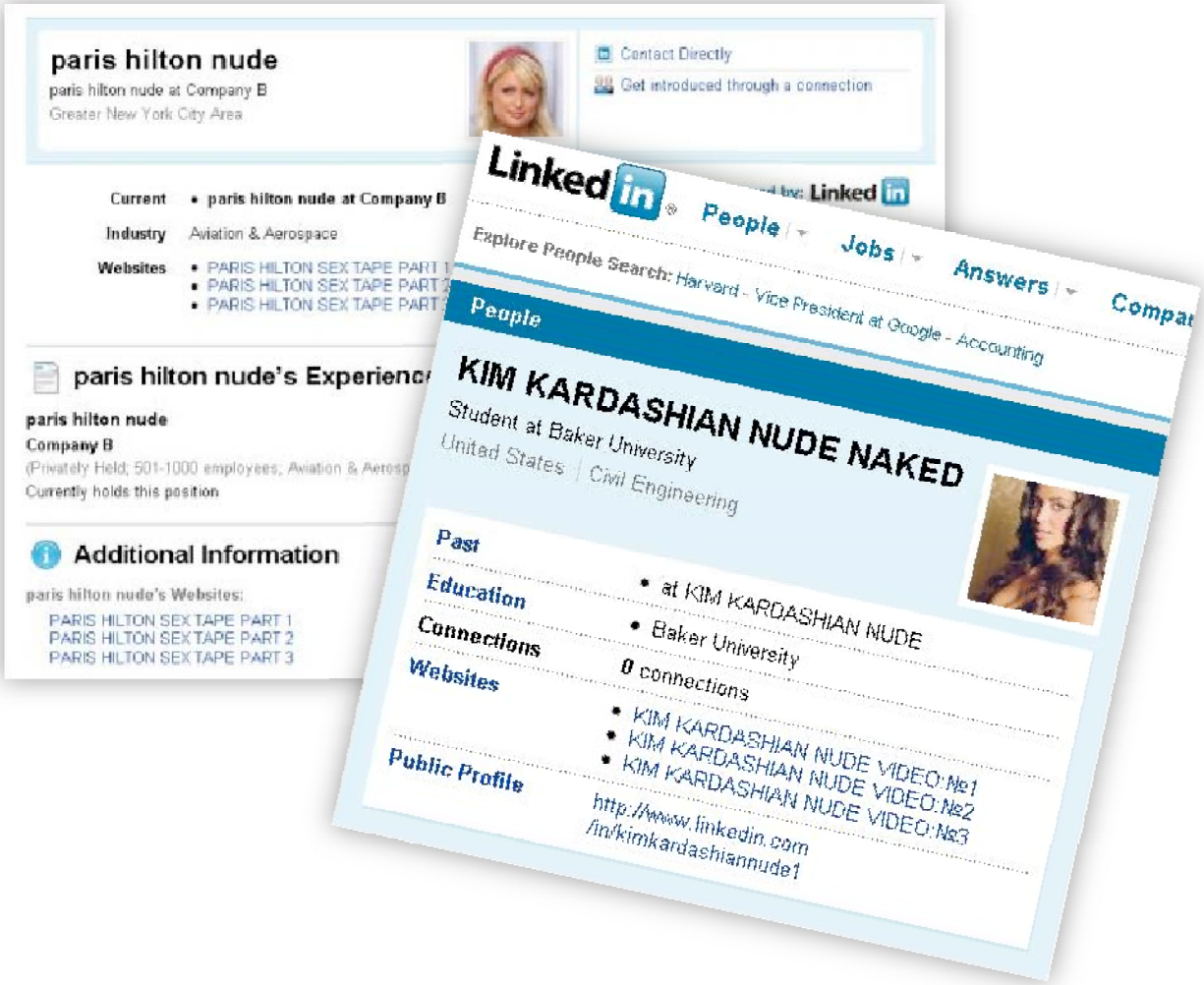
# Social Media Malware

Malicious software, including viruses, trojans, worms and other threats



# Social Media Malware

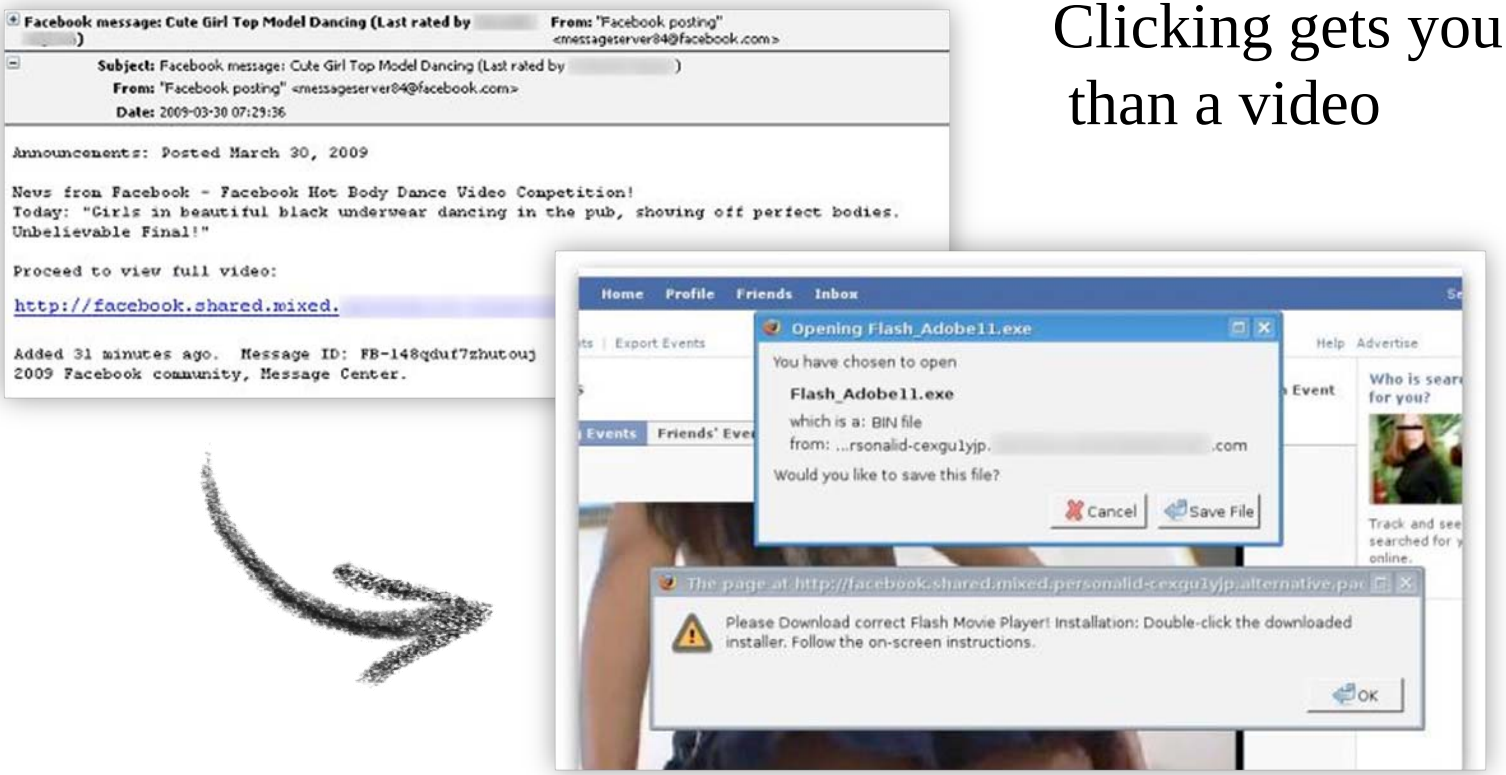
Clicking on the links takes you to sites that will infect your computer with malware




START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Malware

Clicking gets you more than a video



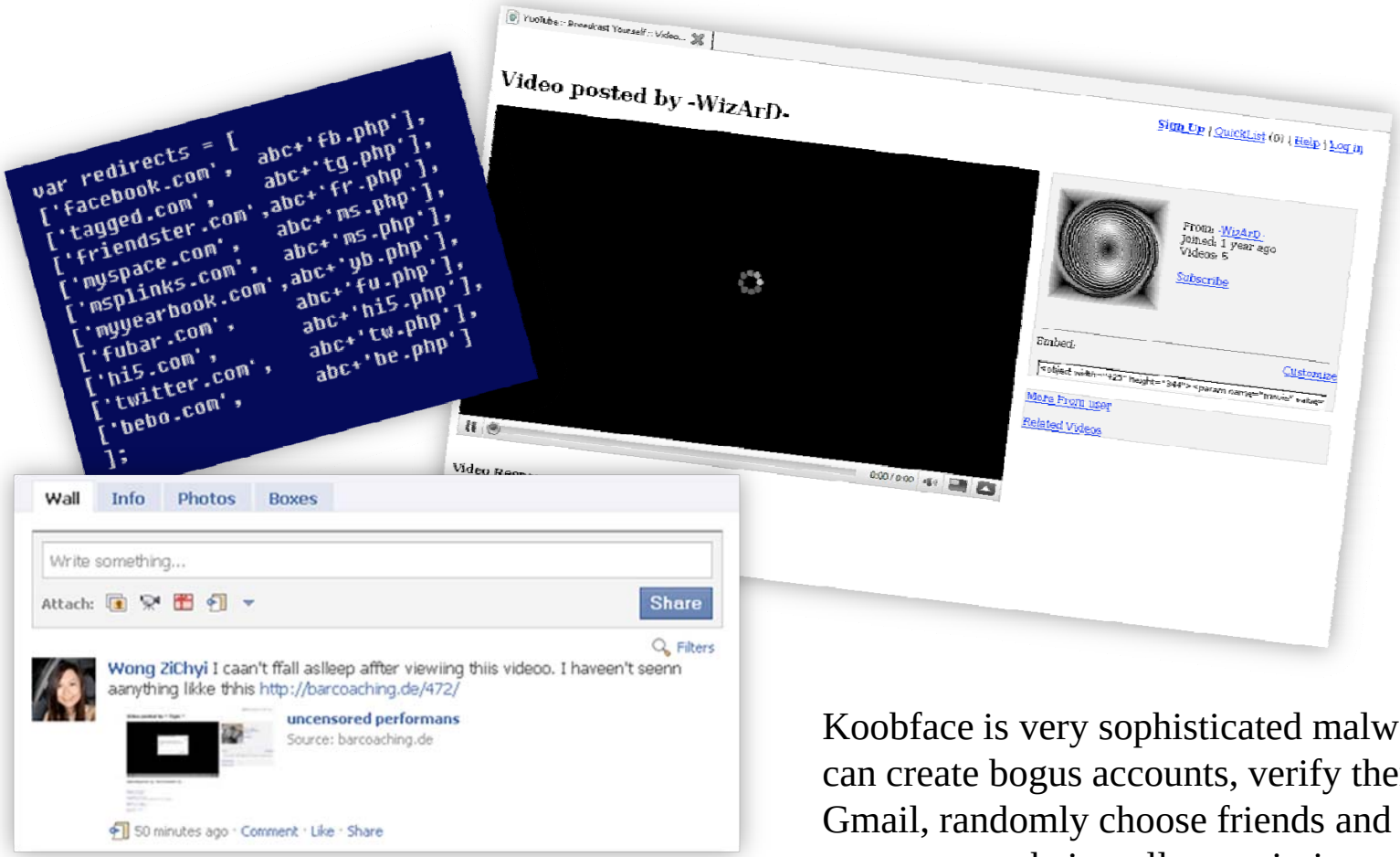

START HERE GO FURTHER FEDERAL STUDENT AID

# Social Media Malware

Clicking gets you
a funny image +
Koobface malware

START HERE
GO FURTHER
FEDERAL STUDENT AID

# Social Media Malware




Koobface is very sophisticated malware. It can create bogus accounts, verify them via Gmail, randomly choose friends and post messages to their walls… pointing (typically) to a malicious video page

START HERE GO FURTHER FEDERAL STUDENT AID

# What Now! (Scared Yet?)

START HERE
GO FURTHER
FEDERAL STUDENT AID

# Top Tips for Staying Secure

- KNOW THE RULES - check your organization's policy on social media
- USE SECURE PASSWORDS - minimum 14 characters including non-letters
- CHECK THE DEFAULT SETTINGS - don't provide personal information by default
- BE PICTURE PRUDENT - think before posting images that might cause embarrassment
- BEWARE OF BIG BROTHER - assume everyone can read your posts, including hackers
- SECURE YOUR COMPUTERS - use up-to-date security software and firewalls
- THINK BEFORE YOU CLICK - if the email looks dodgy, it probably is
- STRANGER DANGER - beware of unsolicited invitations from spammers

# Education is the Key

**QUOTABLE**

"I think this level of awareness and communication needs to start in elementary school, because I'd like to say **everyone is armed today**. Everyone you see has a **cell phone** and a cell phone has an IP address, and every device with an IP address is a **point of entry or intrusion into our network** because we are so well-connected and we communicate so well to each other so therefore we need to start this education as early as possible."

*Zal Azmi, former FBI Chief Information Officer*

START HERE GO FURTHER FEDERAL STUDENT AID

# Helpful Links

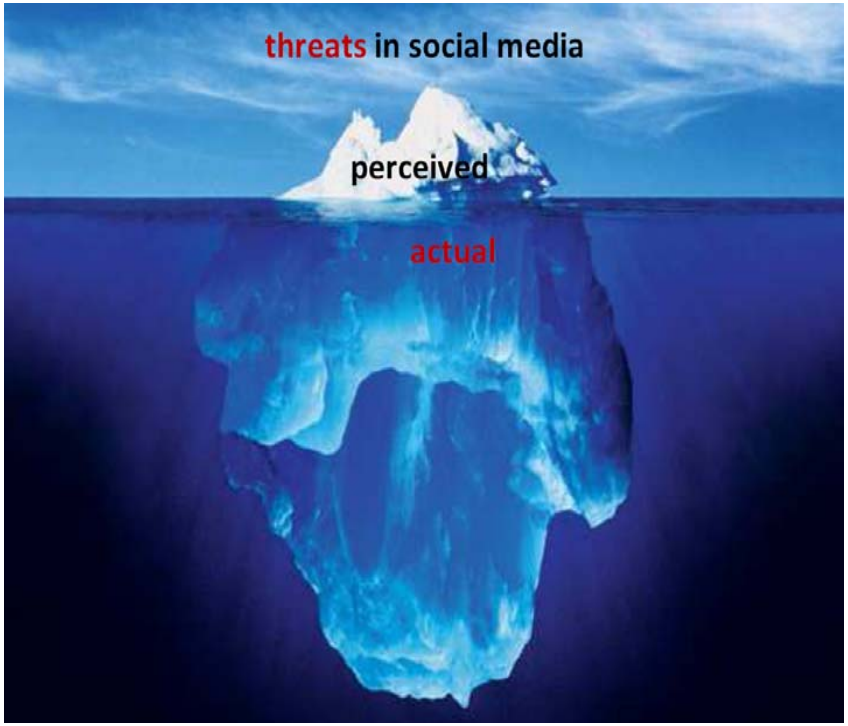
- Links:
  - Federal Trade Commission http://www.ftc.gov/
  - Microsoft Security http://www.microsoft.com/security/default.aspx
  - Sophos - http://www.sophos.com/lp/threatbeaters/download-toolkit/
  - "Own Your Space--Keep Yourself and Your Stuff Safe Online" Digital Book for Teens by Linda McCarthy http://www.microsoft.com/downloads/en/details.aspx?FamilyID=87583728-ef14-4703-a649-0fd34bd19d13
  - Consumer Reports http://www.consumerreports.org/cro/electronics-computers/resource-center/cyber-insecurity/cyber-insecurity-hub.htm
  - StaySafeOnline.org http://www.staysafeonline.org/

# References

- This Presentation was brought to you by:
  - Sophos ThreatBeaters Social Media Toolkit
  - "Seven Deadliest Social Network Attacks" by Cart Timm and Richard Perez
  - "Social Networking Spaces" by Todd Kelsey
  - "Web 2.0 Architectures" by Governor, Hinchcliffe, and Nickull
  - Department of Homeland Security Daily Cyber Security Report
  - Defense Information Systems Agency Security Awareness Course
  - Secure Computing News Wire and other security on-line magazines

# Summary

- The risks from social media are real - for you and for your organization
- Financially-motivated criminals are increasingly using social media sites to steal identities, spread malware and send spam
- Social networks are getting better at protecting users against these threats – but there's a long way to go
- The onus is on **YOU** to use social media sites safely
- Don't stop using social media … just make sure you use it safely!




START HERE GO FURTHER FEDERAL STUDENT AID

# Contact Information

We appreciate your feedback and comments. We can be reached at:

- Phone: 202-377-3893
- Email: Ross.Hughes@ed.gov
- Fax: 202-275-0907

START HERE GO FURTHER FEDERAL STUDENT AID