



# **Staying Safe Online**

## **Protect your Privacy**

**Eric Lukens – ITS Security Office  
University of Northern Iowa**



## Security Office

- The security office in ITS provides assistance and information to all members of the UNI community seeking assistance in making computing more secure.
- Respond to security-related incidents.
- Work to ensure UNI is adequately protecting computer systems.
- <http://www.uni.edu/its/security/>



## About Me

- Eric Lukens
- IT Security Policy and Risk Assessment Analyst
- ITS-Network Services
- [eric.lukens@uni.edu](mailto:eric.lukens@uni.edu)
- [security@uni.edu](mailto:security@uni.edu)
- <http://www.uni.edu/elukens/>



## **This Presentation**

- <http://www.uni.edu/its/security/onlinesafety.html>
  - Links to relevant sites
  - Links to software mentioned
  - Copy of this PowerPoint



## **Why Should I Care**

- Online predators
- Identity theft
- Lost data
- Lost time
- Lost money
- Embarrassment
- Slow computer



**Who are we protecting  
ourselves from?**



## Who?

- Hackers (smallest group by far)
- Curious Individuals
- Illegitimate Businesses
- Semi-legitimate Businesses
- Organized Crime
- Foreign Governments



# Malware



## Reported Attack Site!

---

This web site [REDACTED] has been reported as an attack site and has been blocked based on your security preferences.

---

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#)

[Why was this site blocked?](#)

[Ignore this warning](#)





## Malware

- **MAL**icious soft**WARE**
- A catch-all term
- Virus, rootkit, trojan, worm, spyware, adware, etc.
- It is stuff you don't want on your computer



# How Malware Enters Comp.

- Traditional, but still work
  - Email
  - Dirty files from other computers
  - Worms (self-spreading via security vulnerabilities)
- Modern
  - “Dirty” websites
  - Flash drives
  - Bundled “extras” in software downloads
  - Browser exploits



## Traditional Prevention

- Don't open email attachments you weren't expecting
- Don't trust files from computers or people you don't know or trust

Not Good Enough



## Modern Prevention

- Traditional prevention
- Up-to-date software
- Download and install software only from websites you know and trust
- Run anti-malware software
  - Typically still called anti-virus software
- Stop. Think. Click. while browsing
- You are the most important part of keeping malware off your machine



## Anti-Malware Software (Windows)

- Plenty in the stores, most of those are fine.
- Free ones as well, they work fairly well.
  - Avast
    - <http://www.avast.com/>
  - AntiVir
    - <http://www.free-av.com/>
  - Microsoft Security Essentials
    - [http://www.microsoft.com/security\\_essentials/](http://www.microsoft.com/security_essentials/)
  - AVG Free has problems, paid versions are fine.
- Non-commercial use only



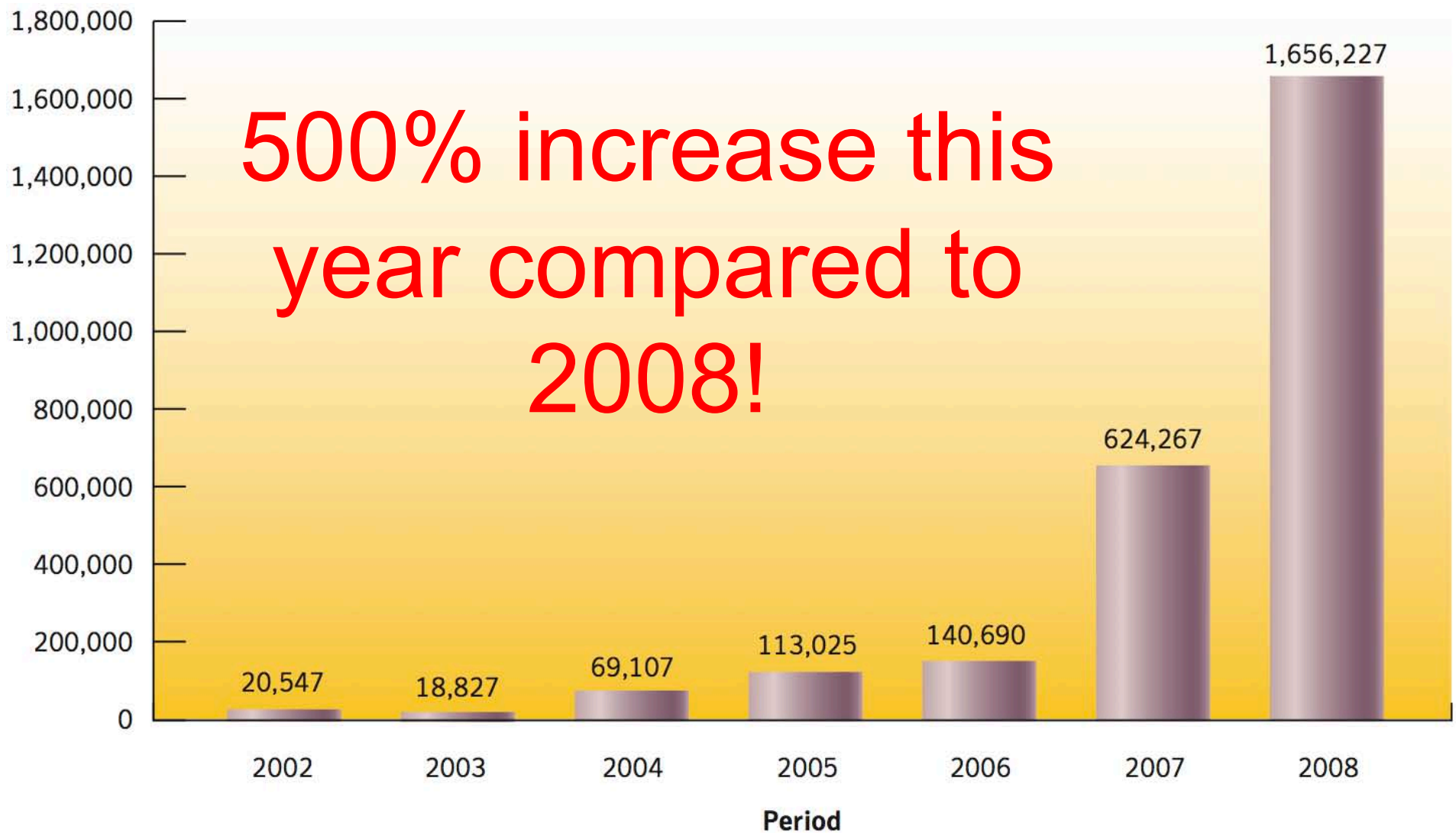
## Additional Protection (Windows)

- In addition to typical anti-malware software, you can run these additional on-demand scanners.
  - Malwarebytes
    - <http://www.malwarebytes.org/>
  - Spybot Search and Destroy
    - <http://www.safer-networking.org/en/index.html>
  - Ad-Aware
    - <http://www.lavasoft.com/>
- These scanners can pick up stuff your normal A/V misses.



## **Anti-Malware not keeping-up**

- Last couple years have seen exponential increase in the numbers of malware.
- New variants released hourly.
- Anti-malware software like vaccine, it can only prevent known, common infections.
- Bad guys always looking for new ways to trick you.

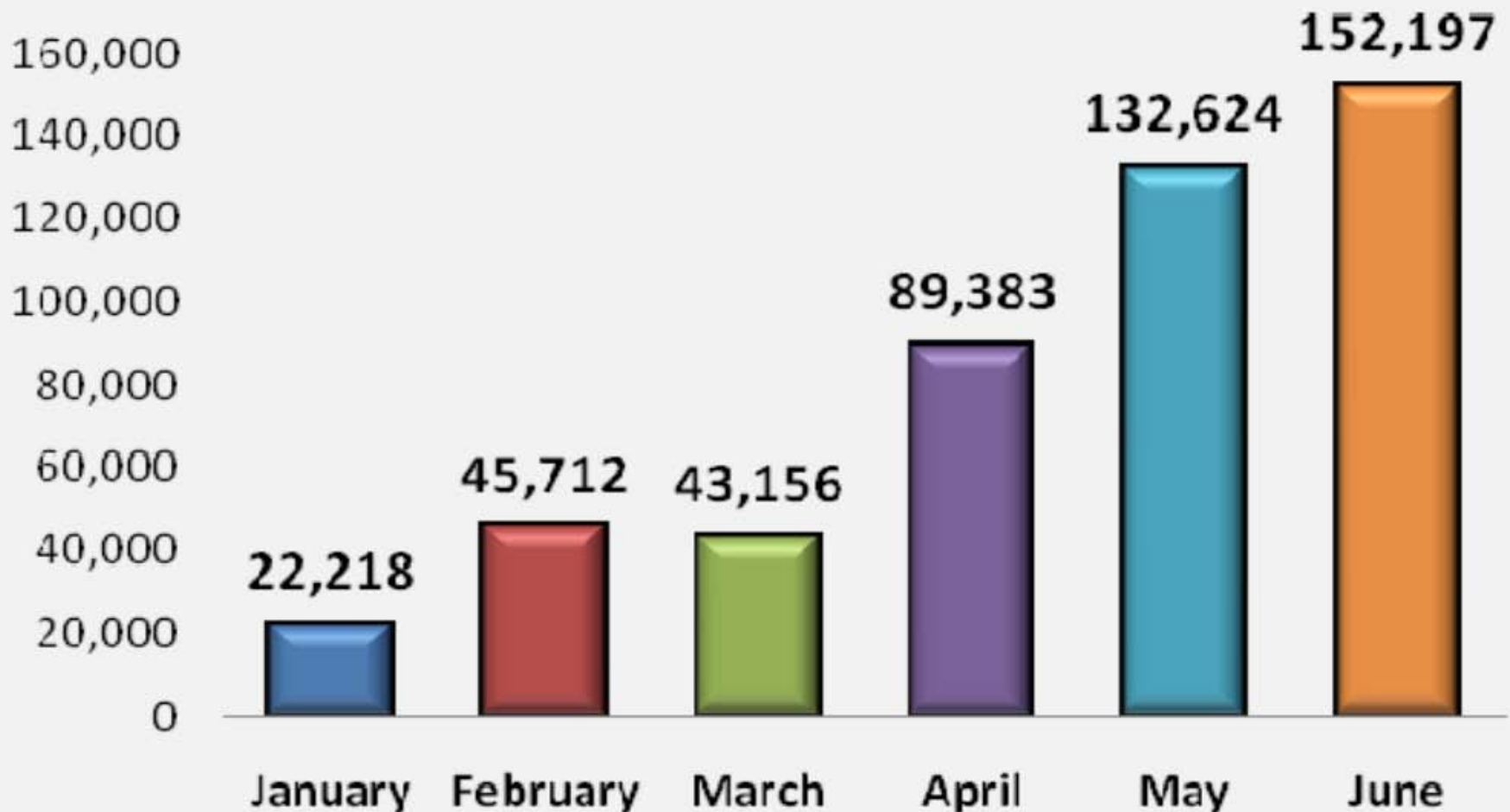


**Figure 3. New malicious code threats**

*Source: Symantec*



## Rogue Anti-Malware Programs 1st Half '09





## Browse at your own risk

- Exploits and problems have made “good” sites evil
- Good news, with good security settings you usually have a chance to stop it. You’re usually going to have to approve the install of malware.
  - Not always true in the case of exploits.



## **Stop. Think. Click.**

- Does what's popped up on the screen make sense?
- Research or ask if in doubt
- Closing the browser and starting your web journey over again is probably a safe bet if your doubtful.



# Antivirus 360

Online Security Scanner

now scanning: complete

items processed: 1100

ERRORS FOUND: 46

**Microsoft Security Warning**

Antivirus 360 Web Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	<b>CRITICAL</b>
Zlob.PornAdvertiser.Xplisit	Spyware	<b>High</b>
Trojan.InfoStealer.Banker.s	Trojan	<b>Medium</b>

Remove All    Ignore

#	Threat Name	Items Infected
1	Trojan.Mytob.Mai	69
2	Trojan.Zlob.z	4
3	Worm.Apache.x	0

XP online security scanner has detected and removed Malware threats from your computer. Failed to delete **critical level threats** - in order to remove them we recommend you to install XP antivirus protection for free

Remove Threats

antispy software for Windows XP

Copyright © 2007 - 2008 Antivirus 360 | All Rights Reserved

# Mac



# Your Browser

- [Microsoft Internet Explorer](#)
  - [Mozilla Firefox](#)
  - [Apple Safari](#)
  - [Google Chrome](#)
  - [Opera](#)
- 
- They all have exploits. The more common, the more they are exploited. Cat and mouse game, but it does work.



## Warning: Visiting this site may harm your computer!

The website at [redacted] contains elements from the site [redacted], which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

For detailed information about the problems with these elements, visit the Google [Safe Browsing diagnostic page](#) for [redacted].

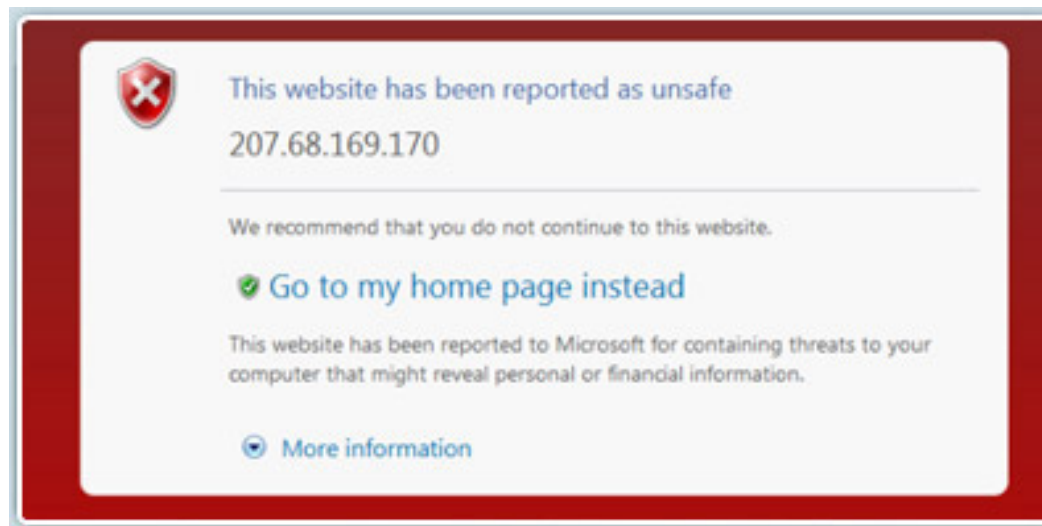
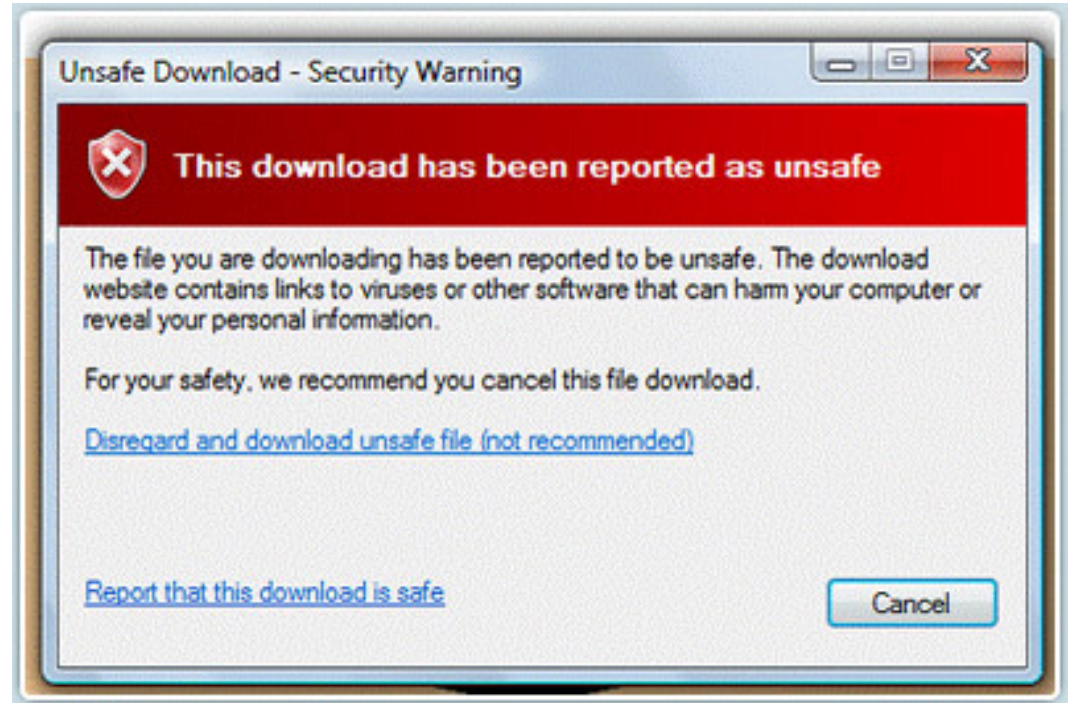
[Learn more about how to protect yourself from harmful software online.](#)

I understand that visiting this site may harm my computer.

Google Chrome



# IE 8





## Plug-ins

- Every browser uses plugins, some are common across platforms and browsers.
  - Java
  - Adobe Flash Player
  - Adobe Reader
  - QuickTime/Real Player
- Use these programs built-in update features and don't ignore them.





## **Automatic Updates**

- Windows Update
- Apple Software Update
- Check them regularly and do as they prompt.
- Do not disable them, do not put off their patches.
- Same with other programs.



## Backups

- If the read/write head of a hard-disk were a Boeing 747, and the hard-disk platter were the surface of the Earth:
  - The head would fly at Mach 800
  - At less than one centimeter from the ground
  - And count every blade of grass
  - Making fewer than 10 unrecoverable counting errors in an area equivalent to all of Ireland.



## Backups (For Home Only)

- Many ways to backup data, depends on your particular needs.
  - Flash drives
  - [Mozy](#) (2GB Free)
  - External Hard Drives
- So many ways to lose your data, you need backups.
- Keep backups in a safe location



## **Phishing**

- “Fishing” for information
- The “Ph” makes it cool.



## Phishing

- Don't email personal or financial information—ever. Any legitimate entity that asks you to needs to change their business practices.
- Don't reply to email or pop-up messages that ask for personal or financial information, and don't click on links in the message.
- Never provide your passwords to anyone. UNI will not ask for them, nobody else should either.



## Phishing

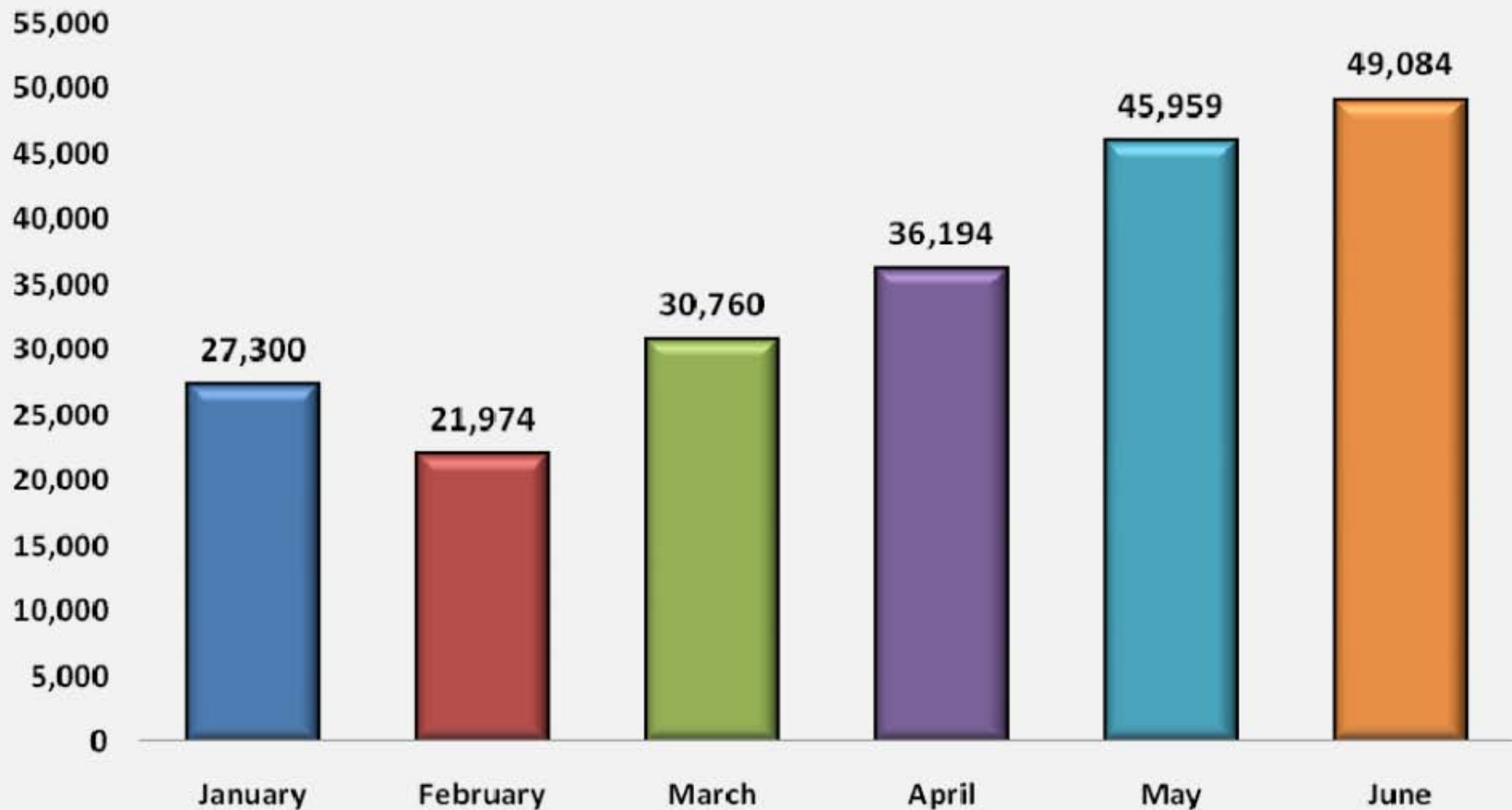
- If it sounds too good to be true, it probably is.
- Use sound judgment. Ask yourself if a particular request received makes sense.
- While not universal trait, many phishing attempts include poor spelling and grammatical errors.
- Be very suspicious of any request to “verify your information.”



## Phishing

- Note the URL of websites you visit before providing information.
- If unsure, call using known good source or visit site directly using known good link.
- [phishing@uni.edu](mailto:phishing@uni.edu)
  - For reports of phishing emails that make it to UNI email accounts

## Unique Phishing Site Detected January - June '09







## **Passwords**

- The keys to the kingdom
- Only thing that stops people from getting into your stuff.



## Passwords

- Passphrases are better if you can use them
  - My cat Willow demands food at 5:00AM.
- Creative passwords
  - Ittr@b0htrbikfa
  - I'm trying to read a book on how to relax, but I keep falling asleep.



## Bad Passwords

- 1Letmein!
- P@ssw0rd
- Qqqqqq\$1
- P@nathers1
- Password crackers are very fast at cracking common passwords.
- Avoid words, even with variations.
- Some password systems can be cracked faster than others.
- Security questions help.
- Different passwords on different systems



## **Privacy Online**

- Keep some things to yourself
- Research and be smart
- Nothing ever goes away on the internet
- Avoid using public computers
- Extra caution when using your computer in a wireless "hot spot"



## Privacy Online

- Familiarize yourself with your websites
  - Be cautious when changes appear
- SSNs, DLs, bank account #'s should rarely be typed online

# HTTPS

- Look for the lock and the “S”
- This means information between you and the site on the other end can't be intercepted on its way there and back.
- Anyone can get an HTTPS site.
- New Extended Validation certificates can verify identity as well.





## Online Shopping

- Know who you're dealing with
  - Research
- Know exactly what you're buying
- Know what it will cost
- Pay by credit card
- Check out the terms of the deal
- Save records of your online transactions



## Online Banking

- Remember the phishing tips
- Protect your passwords
- Follow your bank's advice
- Turn to unbiased sources when researching investments
- Don't let your browser "remember" your username and password information
- Careful with taxes online





# Identity Theft

- <https://www.annualcreditreport.com>
  - Not the other one with catchy tunes
- Check credit report annually for problems
- Always read account statements
- Report problems immediately to the account provider and the credit reporting agencies to put a fraud alert on your file
- Police report/report to FTC



## Get anything you want

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	\$0.06-\$30
2	2	Bank account credentials	19%	17%	\$10-\$1000
3	9	Email accounts	5%	4%	\$0.10-\$100
4	3	Email addresses	5%	6%	\$0.33/MB-\$100/MB
5	12	Proxies	4%	3%	\$0.16-\$20
6	4	Full identities	4%	6%	\$0.70-\$60
7	6	Mailers	3%	5%	\$2-\$40
8	5	Cash out services	3%	5%	8%-50% or flat rate of \$200-\$2000 per item
9	17	Shell scripts	3%	2%	\$2-\$20
10	8	Scams	3%	5%	\$3-\$40/week for hosting, \$2-\$20 design

**Table 1. Goods and services available for sale on underground economy servers**

Source: Symantec



## Signs of ID Theft

- Unusual or unexplainable charges on your bills
- Phone calls or bills for accounts, products, or services that you do not have
- Failure to receive regular bills or mail
- New, strange accounts appearing on your credit report
- Unexpected denial of your credit card



## **Social Networking**

- Should the info really be disclosed?
- Consider everything you post on a social networking site as being accessible to everyone
  - Employers
  - Coworkers
  - Family
  - Law Enforcement



## **Social Networking**

- Use the privacy settings
- Myspace has poor privacy settings
- Facebook has gotten better
- Do not post information about your day-to-day schedule
- Check the site daily to remove content you don't want to be associated with.



## **Social Networking**

- Avoid the camera
- Don't do things that would get you in trouble
- Be kind to your friends and they'll (hopefully) be kind in return



- Unless you're promoting your band, only allow friends.
- Only post information you want everyone to see.
- Its pretty much everyone or just friends.
- Think of MySpace as a website.

# MySpace Privacy Settings

## General Privacy:

---

**Online Now:**  Show people when I am online

**Birthday:**  Show my birthday to my friends

**Profile Viewable By:**  Everyone  
 Everyone 18 and over  
 My friends only

**Comments:** Choose who can view [your comments page](#).

- Anyone can view my comments page  
 Anyone 18 and over can view my comments page  
 Only my friends can view my comments page

**Friends:** Choose who can view [your friends page](#). Mutual friends are always public.

- Anyone can view my friends page  
 Anyone 18 and over can view my friends page  
 Only my friends can view my friends page

**Photos:** Choose who can view [your photos page](#). Set album level privacy in photos.

- Anyone can view my Photos page  
 Anyone 18 and over can view my Photos page  
 Only my friends can view my Photos page

Allow my photos to be shared/emailed

**Status and Mood:** Choose who can view [your Status and Mood page](#).

- Anyone can view my Status & Mood page  
 Anyone 18 and over can view my Status & Mood page  
 Only my friends can view my Status & Mood page

**Block Users By Age:**  Allow users under 18 to contact me

**Block Users:** Block individual users by clicking "Block User" on their profile.  
[\[View list\]](#)

Save All Changes



# MySpace Application Settings

[Contact Info](#) | [Account](#) | [Password](#) | [Privacy](#) | [Spam](#) | [Notifications](#) | [Applications](#) | [IM](#) | [Mobile](#) | [Calendar](#) | [Miscellaneous](#)  
[Ad Categories](#) | [No More CAPTCHAs](#) | [Sync](#)

---

## **Apps I've Added**

---

You have no applications installed. Find new applications to install in the [Application Gallery](#).

## **Apps I've Blocked [?]**

---

You have not blocked any applications.

## **Apps I Haven't Added**

---

**Permissions:**  Block apps I haven't added from viewing my display name & public photos [?]

Block apps I haven't added from communicating with me [?]



- Granular privacy settings
- Can be a bit tricky to master them
- Still, assume everything can be seen by everyone



### Profile ▶

Control who can see information on your profile page.



### Search ▶

Control who can search for you, what they can see, and how they can contact you.



### News Feed and Wall ▶

Control what Recent Activity is visible on your profile and in your friends' home pages.



### Applications ▶

Control what information is available to applications you use on Facebook.

#### Block People

If you block someone, they will not be able to find you in a Facebook search, see your profile, or interact with you through Facebook channels (such as Wall posts, Poke, etc.). Any Facebook ties you currently have with a person you block will be broken (for example, friendship connections, Relationship Status, etc.). Note that blocking someone may not prevent all communications and interactions in third-party applications, and does not extend to elsewhere on the Internet.

#### Block Email

If you cannot find someone to block you can block an email address. We will block any account associated with this email address currently or at any time in the future.

#### Block List

You have not added anyone to your Block list.

##### Person

Block

##### Email



Block



## Privacy ▸ Profile

Basic **Contact Information**



Control who can see which sections of your profile. Visit the [Applications](#) page in order to change settings for applications. Visit the [Search Privacy](#) page to make changes to what people can see about you if they search for you.



See how a friend sees your profile:

**Profile**  Custom  [?]


-  Friends of Friends
-  UNI



[Edit Custom Settings](#)



**Basic Info**  Custom  [?]

-  Friends of Friends
-  UNI



[Edit Custom Settings](#)



**Personal Info**  Friends of Friends  [?]

**Status and Links**  Custom  [?]



-  Friends of Friends
-  UNI

[Edit Custom Settings](#)

**Photos Tagged of You**  Custom  [?]

-  Friends of Friends
-  UNI

[Edit Custom Settings](#)  
[Edit Photo Albums Privacy Settings](#)

**Videos Tagged of You**  Only Friends  [?]

🔒 Privacy ▶ Profile

Basic **Contact Information**

Control who can see your contact information. Visit the [Applications](#) page in order to change settings for applications.

See how a friend sees your profile:

**IM Screen Name** 🔒 Custom ▼  
Friends of Friends  
UNI

[Edit Custom Settings](#)

**Mobile Phone** 🔒 Friends of Friends ▼

**Other Phone** 🔒 Only Friends ▼

**Current Address** 🔒 Friends of Friends ▼

**Website** 🔒 Everyone ▼

**Residence** 🔒 Friends of Friends ▼

**[Redacted]** 🔒 No one ▼

**[Redacted]** 🔒 Custom ▼  
Friends of Friends  
UNI

[Edit Custom Settings](#)


Save Changes

Cancel

 **Privacy** ▶ **Search**

**Search Discovery**

Use this setting below to control who on Facebook can find you through search. Your Friends will always be able to find you.

Search Visibility 

[Edit Custom Settings](#)

**Search Result Content**

People who can find you in search can click through to a very limited version of your profile. Use these checkboxes to control what people can see in addition to your name.

People who can see me in search can see:

- My profile picture
- My friend list
- A link to add me as a friend
- A link to send me a message
- Pages I am a fan of

**Public Search Listing**

Use this setting to control whether your search result is available outside of Facebook.

- Create a [public search listing](#) for me and submit it for search engine indexing ([see preview](#))

Please note that minors do not have public search listings - listings created by minors will activate only when they are no longer minors.

Save Changes


Cancel

🔒 Privacy ▶ News Feed and Wall

Actions within Facebook

Facebook Ads

Posting to someone's Wall may appear in your mutual friends' News Feeds.

  Show Wall posts

The Highlights section on your friends' home pages can include your Recent Activity. Allow Highlights to show my activity when I...

- Comment on or like a note
- Comment on or like a photo or album
- Comment on or like a video
- Comment on or like a link
- Change relationship status

Recent Activity will appear on your Wall when you edit your profile. Also show Recent Activity when I...

- Remove profile info
- Post on a discussion board
- Add a friend

Save Changes

Cancel

Recent Activity will **never** be shown about:

- Pokes
- Messages
- Whose profile you view
- Whose photos you view
- Whose notes you read
- Groups and Events you decline to join
- People you reject as friends
- People you remove from your friends
- Notes and photos you delete

### Ads shown by third party applications

Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If this is allowed in the future, this setting will govern the usage of your information.

Allow ads on platform pages to show my information to

No one



Save Changes

Cancel

Show my social actions in Facebook Ads to

Only my friends





### What Other Users Can See via the Facebook Platform

When a friend of yours allows an application to access their information, that application may also access any information about you that your friend can already see. [Learn more.](#)

You can use the controls on this page to limit what types of information your friends can see about you through applications. Please note that this is only for applications you do not use yourself:

Share my name, networks, and list of friends, as well as the following information:

- |  |  |
|--|--|
| <input type="checkbox"/> Profile picture                             | <input type="checkbox"/> Events I'm invited to                     |
| <input type="checkbox"/> Basic info <a href="#">What's this?</a>     | <input type="checkbox"/> Photos taken by me                        |
| <input type="checkbox"/> Personal info (activities, interests, etc.) | <input type="checkbox"/> Photos taken of me                        |
| <input type="checkbox"/> Current location (what city I'm in)         | <input type="checkbox"/> Relationship status                       |
| <input type="checkbox"/> Education history                           | <input type="checkbox"/> Online presence                           |
| <input type="checkbox"/> Work history                                | <input type="checkbox"/> What type of relationship I'm looking for |
| <input type="checkbox"/> Profile status                              | <input type="checkbox"/> What sex I'm interested in                |
| <input type="checkbox"/> Wall  | <input type="checkbox"/> Who I'm in a relationship with            |
| <input type="checkbox"/> Notes                                       | <input type="checkbox"/> Religious views                           |
| <input type="checkbox"/> Groups I belong to                          | <input type="checkbox"/> Website                                   |

Do not share any information about me through the Facebook API

### Applications Authorized to Access Your Information

When you authorize an application, it can access any information associated with your account that it requires to work. Contact Information is never shared through Platform. You can view a full list of applications you have authorized on the [Applications](#) page.

### Facebook Connect Applications

Facebook Connect is a way to use applications outside of Facebook. You can take your Facebook profile information all over the Internet, and send interesting information back to your Facebook account.

When your friend connects their Facebook account with an application outside of Facebook, they will be able to compare their Facebook Friend List with information from that website in order to invite more friends to connect.

Don't allow friends to view my memberships on other websites through Facebook Connect.

### Beacon Websites

Don't allow Beacon websites to post stories to my profile. [Learn more.](#)

### Blocked Applications

You have blocked the following applications. This means they cannot access any information about you or contact you, but they may still appear on your friends' profile. If you want to remove the block for any of these applications, click remove.

## Edit Photo Album Privacy

### Who Can See This?

Everyone on Facebook

#### Friends

Friends of Friends  
My friends and their friends can see this.

Only Friends  
Only friends can see this.

Some Friends  
Choose specific friends who can see this.

Only Me  
Only you and selected networks can see this.

#### Networks

All of My Networks

#### Except These People

Type the name of a friend or friend list...

Okay

Cancel



# Fake Facebook



### Flash Player upgrade required

You must download and install the latest version of the Adobe Flash Player to view this content.

Download Flash

## Welcome to Video

Your life in motion.

### Share your personal videos.

Upload and tag videos of you and your friends on Facebook. [Upload a new video](#)

### Record and send video messages.

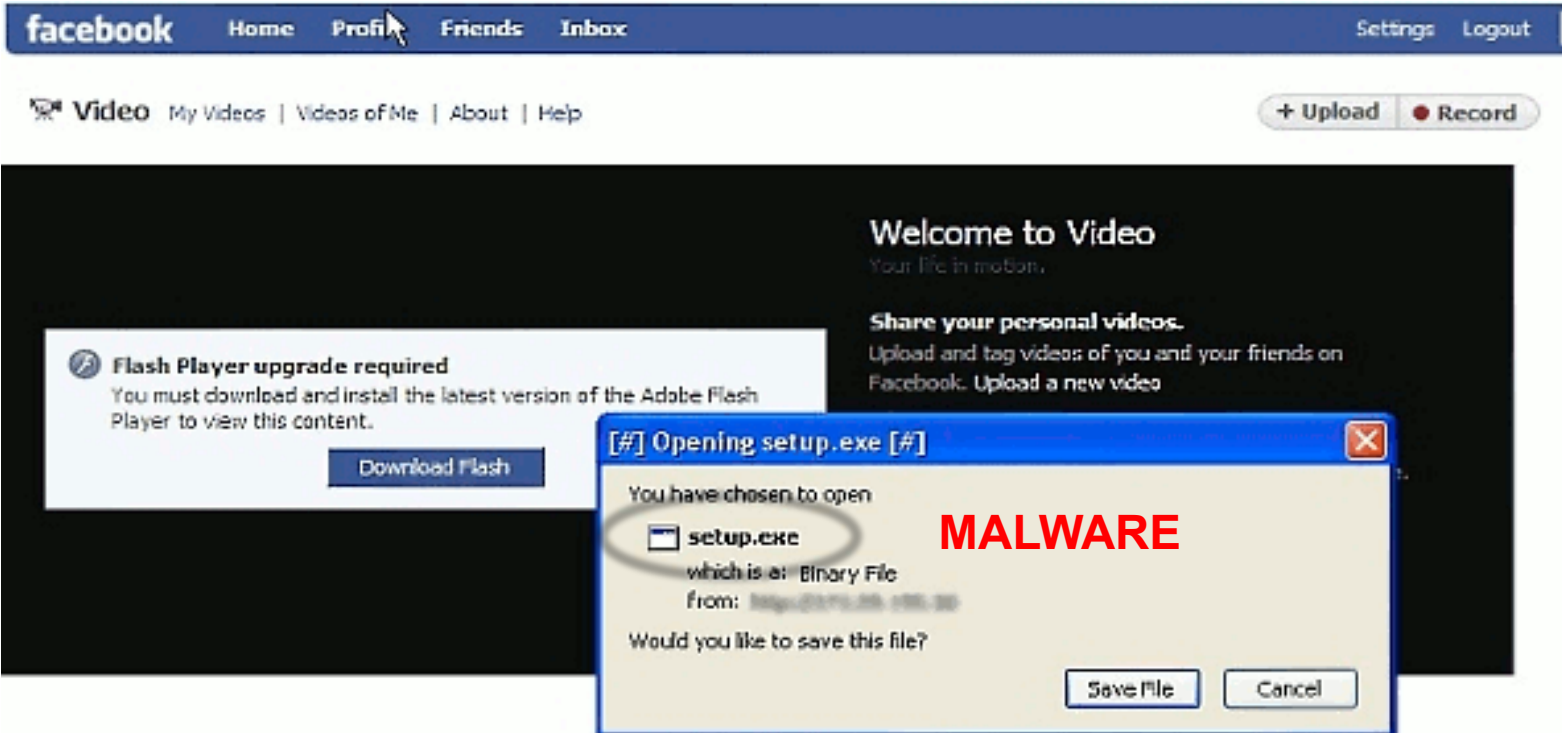
Use your webcam to record yourself in a video message. [Record a video message](#)

### Publish videos from your mobile.

Send mobile videos via email or MMS to your [personal upload address](#).



# Fake Facebook



facebook Home **Profile** Friends Inbox Settings Logout

Video My Videos | Videos of Me | About | Help + Upload Record

Welcome to Video  
Your life in motion.

Share your personal videos.  
Upload and tag videos of you and your friends on Facebook. Upload a new video

**Flash Player upgrade required**  
You must download and install the latest version of the Adobe Flash Player to view this content.  
Download Flash

[#] Opening setup.exe [#]  
You have chosen to open  
**setup.exe**  
which is a: Binary File  
from: [http://www.ck...](#)  
Would you like to save this file?  
Save file Cancel

**MALWARE**



## More Information

- <http://www.onguardonline.gov/>
- <http://www.us-cert.gov/>
- <http://www.staysafeonline.org/>
- <http://www.lookstoogoodtobetrue.com>
- <http://getnetwise.org/>
- <http://www.uni.edu/its/security/>



**Questions?**