Security Seminar

Brian Epstein, MS, CISSP, GIAC
Computer Manager, Network and Security
Information Security Officer

security@ias.edu

https://security.ias.edu

Twitter: @epepepepep
• Three principles of Information Security
  – Availability
  – Integrity
  – Confidentiality
• What is the office of Network Security?
What is the office of Network Security?
IAS Security Structure
• Defense in Depth (IAS Security Structure)
• How do we protect you?
  – Moat
  – Outer ward
  – Middle ward
  – Inner ward

-- Harlech Castle, Gwynedd, North Wales
• How do we protect you?
  – Intrusion Detection (watchtower)
  – Firewall (guard)
  – Intrusion Prevention (customs agent)
    • Spam filter
    • Email virus filter and attachment blocker
    • Anomaly protection
Security Awareness
• October: CyberSecurity Awareness Month
• Seminars
• Website - https://security.ias.edu
• Bulletins
• Posters
• One on one
Strategies to Safer Computing
• Keep your devices up to date
• Choose good passwords, use two factor
• Anti-Malware (virii, trojans, spyware, bots)
• Stop. Think. Connect.
  – email
  – instant message
  – Facebook, Twitter, Instagram, SnapChat
• Privacy/Phishing/Scam Awareness
2014 Tech Obituaries
Windows XP and Office 2003

Total Matches By Year

# of Vulnerabilities Meeting Specified Limitations

Year
Actions for Windows XP and Office 2003

- Upgrade to Windows 8.1
- Install Linux (free)
- Buy a new computer
- Upgrade to Office 2010 or 2013
- Install LibreOffice (free)
Java in the browser
Java in the browser

Exploitation of Application Vulnerabilities
December 2013

- Oracle Java: 50%
- Adobe Acrobat Reader: 15%
- Internet Explorer: 4%
- Google Chrome: 9%
- Others: 22%

source: IBM Security Trusteer research team
Actions for Java in the browser

- If you don't need it, uninstall it (all versions).
- If you don't know, uninstall it. You can always re-install if you find out you were wrong.
- If you do need it, limit it to only the sites that are necessary by using the security settings in the Java Control Panel.
- Notify your site that you'd like them to move to HTML5.
Flash
Actions for Flash

- If you don't need it, uninstall it.
- If you don't know, uninstall it. You can always re-install if you find out you were wrong.
- If you do need it, consider using a browser plugin like FlashBlock (available for Firefox and Chrome).
- Notify your site that you'd like to see them move to HTML5.
Internet Explorer

Internet Explorer release to patch timeline

Days to First Patch

Fig: How long from the GA release of Internet Explorer until the first patch is released?
Actions for Internet Explorer (IE)

- Move to a new browser. The most popular choices are Firefox or Google Chrome.
- When you migrate, take your bookmarks with you, but leave all the rest behind.
- If your site requires IE, considering using IE only for that site.
- Ask your vendor to support other browsers, like Firefox and Google Chrome.
Privacy
• Oct 2013 - PF Chang's
• Nov 2013 – CorporateCarOnline (850k PII)
• Dec 2013 - Target (40m CC, 70m PII)
• Jan 2014 - Michaels (2.6m) & Nieman Marcus (1.1m)
• Feb 2014 - Sears
• Mar 2014 - Experian (200m) & Sally Beauty (280k) & CA DMV
• Apr 2014 - Community Health Systems (millions)
• May 2014 - eBay (145m passwords)
• Jun 2014 - Acme (and other supermarkets)
• Jul 2014 - UPS
• Aug 2014 - JP Morgan Chase (76 million)
• Sep 2014 - Home Depot & Dairy Queen
• Oct 2014 - Kmart
Actions for Privacy

- Monitor your credit score
- Look at your credit report (free in some states)
- Cancel unused credit accounts
- Account for all credit card charges
- Use separate passwords for every account
- Use Two Factor Authentication when possible (more on this later)
Passwords
Passwords Two factor authentication
<table>
<thead>
<tr>
<th>Banking</th>
<th>Docs</th>
<th>SMS</th>
<th>Phone Call</th>
<th>Email</th>
<th>Hardware Token</th>
<th>Software Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ally Bank</td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Altra Federal Credit Union</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>America First Credit Union</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>American Express</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Bank of America</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barclays</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Barclays US</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BMO Harris Bank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boeing Employee Credit Union</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capital One</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capital One 360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chase</td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIBC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**In Progress**: IN PROGRESS!

**Thank You**: THANK THEM FOR WORKING ON 2FA
Actions for Passwords

- Use two factor authentication everywhere you can.
- Ask your bank/healthcare provider/social media site/etc to support two factor authentication.
- Use a password safe (there is a list on https://security.ias.edu)
- Use long passwords or passphrases. Remember, 12 characters is the absolute minimum.
- Classify how strong your password needs to be. Your bank, super strong. Your Twitter account, maybe not.
Magstripe Credit Cards

Smart Chip
-or-
"Embedded Integrated Circuit"
Actions for Magstripe Credit Cards

• Request a chip and pin credit card from your credit card company

• Learn how to use this technology, it's not hard.

• Recognize where it is available, and use it.

• Request your local grocery/pharmacy/retail store to install new readers (and turn them on).
Don't Panic, know your meme
What is “the cloud”? 

Somebody else's computer
How do I delete from “the cloud”? 

You don't. 
It's somebody else's computer.
Heartbleed, Shellshock, POODLE
Actions for Heartbleed, #shellshock and POODLE

- Heartbleed – not much unless you are a WebAdmin
  - If you are https://filippo.io/Heartbleed/
- #shellshock – not much unless you are a SysAdmin
  - If you are https://shellshocker.net/
- POODLE – ah, something to do!
  - Upgrade your browser
  - Test your browser http://poodletest.com
  - Disable outdated encryption
• How to spot a scam
  – Check the sender
  – Do you have an account with them?
  – Do the links make sense?
  – Check on-line urban legend databases.
  – Does it sound too good to be true?
  – Does it sound too bad to be true?
The real card reader slot.

The capture device.

The side cut out is not visible when on the ATM.
As part of our security measures, we regularly screen activity in the PayPal system. During a recent screening, we noticed an issue regarding your account.

Case ID Number: PP-394-509-731

PayPal is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Log In into your account to resolve the problem.

Click here to Log In

Case ID Number: PP-394-509-731
As part of our security measures, we regularly screen activity in the PayPal system. During a recent screening, we noticed an issue regarding your account.

Case ID Number: PP-394-509-731

PayPal is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Log in into your account to resolve the problem.

Click here to Log In

Case ID Number: PP-394-509-731

Copyright © 1999-2008 PayPal. All rights reserved.
PayPal Email ID PP572
Dear Commerce Bank customer:

Commerce Bank Customer Service requests you to complete Commerce Connections Form.

This procedure is obligatory for all business and commercial customers of Commerce Bank.

Please select the hyperlink and visit the address listed to access Commerce Connections Form.

http://commerceconnections.commercebank.com/cmsserver/ccf.cfm?session=1047830511608772100442415154861818520580714371832

Again, thank you for choosing Commerce Bank for your business needs. We look forward to working with you.

This mail is generated automatically.

Commerce Bank Customer Service
• Strategies for families
  – Supervise children
  – Create a different, unprivileged account for each family member
  – Don't share passwords
  – Don't give access to critical computers
  – Scan now, scan often and install updates
  – Teach your family to protect their information
  – Contact your helpdesk!
Policies to Protect You
- Wireless access points (a.k.a. rogues)
- Illegal file sharing
- Infected computers
- Network access is a privilege
- We are here to help
Resources for you
• Free anti-virus for Windows
• Free tools to secure your computer
• Free password safes
• Free advice on protecting yourself

all this and more . . .

https://security.ias.edu
Questions?

security@ias.edu
Copyrights


Harlech Castle Aerial Photos -

Crown Copyright: Royal Commission on the Ancient and Historical Monuments of Wales

Hawlfraint y Goron: Comisiwn Brenhinol Henebion Cymru

http://www.rcahmw.gov.uk/LO/ENG/About+Us/Terms+and+Conditions/Copyright/

Harlech Castle Layout - Oman, Charles: “Castles” (1926), stock image royalty-free for non-commercial uses only, usage credit requested

Aloha! Postcard - © 2008 Institute for Advanced Study
Security Seminar

Brian Epstein, MS, CISSP, GIAC
Computer Manager, Network and Security
Information Security Officer
security@ias.edu
https://security.ias.edu
Twitter: @epepepep

My role at the IAS is to ensure availability and security of our network to enable our Faculty, Members, Visitors and Staff to access the resources they need.
• Three principles of Information Security
  - Availability
  - Integrity
  - Confidentiality

These principles are shown here in the IAS Security Logo.

Each of these principles is important, although we do prioritize them in an order appropriate for the IAS.

Available of resources is first. We are not a bank or a corporate office, so we need to ensure our scholars have access to the resources they need.

Integrity ensures that the information we receive is correct and confidentiality ensures it is shared only with intended audiences.
What is the office of Network Security?

In my experience, a network and security officer is often regarded as a roadblock to productivity as represented by this red light.

I would like to change this misconception by redefining the position as a ...
What is the office of Network Security?

... yellow light.

Proceed, but with caution
IAS Security Structure

How do we structure our network to protect you?
Defense in depth is not a new concept, it has been around for many centuries or longer.

Our perimeter defenses are similar to that of a castle.
How do we protect you?

- Intrusion Detection (watchtower)
- Firewall (guard)
- Intrusion Prevention (customs agent)
  - Spam filter
  - Email virus filter and attachment blocker
  - Anomaly protection
Security Awareness
Ways to give you information about protecting yourself.
Strategies to Safer Computing
• Keep your devices up to date
• Choose good passwords, use two factor
• Anti-Malware (virii, trojans, spyware, bots)
• Stop. Think. Connect.
  – email
  – instant message
  – Facebook, Twitter, Instagram, SnapChat
• Privacy/Phishing/Scam Awareness

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
2014 Tech Obituaries

We've seen a lot of technology come and go in 2014. Here is a round up of things that left us, or should have left us in 2014.
Patch Tuesday started in 2003 to reduce costs of deploying patches.
Actions for Windows XP and Office 2003

- Upgrade to Windows 8.1
- Install Linux (free)
- Buy a new computer
- Upgrade to Office 2010 or 2013
- Install LibreOffice (free)

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
Python surpassed Java as the number one programming language taught, and it is about time!

The number of Java vulnerabilities over the last year has been outright exhausting.
Actions for Java in the browser

- If you don't need it, uninstall it (all versions).
- If you don't know, uninstall it. You can always re-install if you find out you were wrong.
- If you do need it, limit it to only the sites that are necessary by using the security settings in the Java Control Panel.
- Notify your site that you'd like them to move to HTML5.

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
Steve Jobs announces that HTML5 will win over Adobe Flash in 2010

Adobe announces that it is focusing on HTML5 in 2011

It's now 2014, time to put flash player to rest.
Actions for Flash

- If you don't need it uninstall it.
- If you don't know, uninstall it. You can always re-install if you find out you were wrong.
- If you do need it, consider using a browser plugin like FlashBlock (available for Firefox and Chrome).
- Notify your site that you'd like to see them move to HTML5.

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
Firefox and Chrome are emerging on top in this battle for the browser.
Actions for Internet Explorer (IE)

- Move to a new browser. The most popular choices are Firefox or Google Chrome.
- When you migrate, take your bookmarks with you, but leave all the rest behind.
- If your site requires IE, considering using IE only for that site.
- Ask your vendor to support other browsers, like Firefox and Google Chrome.

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
Privacy
See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
Actions for Privacy

- Monitor your credit score
- Look at your credit report (free in some states)
- Cancel unused credit accounts
- Account for all credit card charges
- Use separate passwords for every account
- Use Two Factor Authentication when possible (more on this later)

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
For those of you that still think Apple Macintosh does not need anti-virus protection...
For those of you that still think Apple Macintosh does not need anti-virus protection...
My new favorite website
Actions for Passwords

- Use two factor authentication everywhere you can
- Ask your bank/healthcare provider/social media site/etc to support two factor authentication.
- Use a password safe (there is a list on https://security.ias.edu)
- Use long passwords or passphrases. Remember, 12 characters is the absolute minimum.
- Classify how strong your password needs to be. Your bank, super strong. Your Twitter account, maybe not.

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
For those of you that still think Apple Macintosh does not need anti-virus protection...
Actions for Magstripe Credit Cards

- Request a chip and pin credit card from your credit card company
- Learn how to use this technology, it's not hard.
- Recognize where it is available, and use it.
- Request your local grocery/pharmacy/retail store to install new readers (and turn them on).

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
All is not lost. We are all in the same boat. The Internet is an invaluable communication tool that has brought the world together.
What is “the cloud”?

Somebody else's computer

Keep yourself aware.
How do I delete from “the cloud”?  

You don't.  
It's somebody else's computer.

Understand the risks of where you store your data.
Heartbleed, Shellshock, POODLE
Actions for Heartbleed, #shellshock and POODLE

- Heartbleed – not much unless you are a WebAdmin
  - If you are https://filippo.io/Heartbleed/
- #shellshock – not much unless you are a SysAdmin
  - If you are https://shellshocker.net/
- POODLE – ah, something to do!
  - Upgrade your browser
  - Test your browser http://poodletest.com
  - Disable outdated encryption

See security website on strategies to pick good passwords which are easy to remember.

Use a password safe for infrequently used passwords.

Apple Macintosh users no longer have an excuse not to use anti-virus software. Free solutions for personal use are available.
• How to spot a scam
  - Check the sender
  - Do you have an account with them?
  - Do the links make sense?
  - Check on-line urban legend databases.
  - Does it sound too good to be true?
  - Does it sound too bad to be true?

Check the sender
Do you have account?
Links make sense?
Snopes
Nigerian scam
Ransomware
Data doctor 2010 . . .
ATM Skimmers are becoming more prevalent
This looks like a legitimate email from PayPal with serious information about my account.

However, when I hover over the like they provide . . .
It turns out it isn't from Paypal at all!

Log directly into your account and look for messages or alerts.

Paypal one time password key fob.

Another great resource is snopes.com. If you receive an email, verify it before sending it on or acting upon it. Here is our favorite Nigerian scam . . .
Notice how Thunderbird warns us that it appears to be a scam.

Then there are the fantastic alerts and pop ups . . .
• Strategies for families
  - Supervise children
  - Create a different, unprivileged account for each family member
  - Don't share passwords
  - Don't give access to critical computers
  - Scan now, scan often and install updates
  - Teach your family to protect their information
  - Contact your helpdesk!

As parents and siblings, we often share with each other ways to protect ourselves.

Look both ways before crossing the street.

Invest your money wisely.

Don't pay sticker price for a used car.

Why not share ways to spot a scam . . .
In order to protect the IAS as a whole, we have introduced policies.
• Wireless access points (a.k.a. rogues)
• Illegal file sharing
• Infected computers
• Network access is a privilege
• We are here to help

Unauthorized access points can cause issues with other users on the network. In general, we ask our users not to install them, and may have to take them down. It also bypasses our wireless security.

DMCA

We will shut down infections before they grow.

IPP – There is a policy, as there are at other institutions.

Cloud services are ok, just be careful.
In order to protect the IAS as a whole, we have introduced policies.
Unauthorized access points can cause issues with other users on the network. In general, we ask our users not to install them, and may have to take them down. It also bypasses our wireless security.

DMCA

We will shut down infections before they grow.

IPP – There is a policy, as there are at other institutions.

Cloud services are ok, just be careful.
Questions?

security@ias.edu

Thank you for your time and patience. Do you have any questions that we can answer?

Please take some materials with you.
Copyrights


Harlech Castle Aerial Photos -

Crown Copyright: Royal Commission on the Ancient and Historical Monuments of Wales
Hawlfraint y Goron: Comisiwn Brenhinol Henebion Cymru
http://www.rcahmw.gov.uk/LO/ENG/About+Us/Terms+and+Conditions/Copyright/

Harlech Castle Layout - Oman, Charles: “Castles” (1926), stock image royalty-free for non-commercial uses only, usage credit requested

Aloha! Postcard - © 2008 Institute for Advanced Study