Management Standards Training 2017

Protecting Yourself & DePaul: Keeping Secrets Secret
(or, Please Don’t Click On That!!)

Session Objectives

- Understand why we are targets
- Recognize and protect ourselves and DePaul from threats
You are a target

What do attackers want?

– usually monetary gain
– access to information that will provide monetary gain
– confidential business or personal information
– revenge
What do you have that they want?

• Account credentials to:
  – Financial accounts
  – Other service providers: iCloud, Google Drive, Dropbox, Box
  – Amazon or other shopping

• Identity theft potential
  – Social media accounts
  – Email accounts
And....

- Financial Information
  - Credit cards / ProCards
  - Tax records
  - Bank accounts
Credit Cards for Sale

![Image of credit card dump website]

<table>
<thead>
<tr>
<th>Bin</th>
<th>Card</th>
<th>Debit/Credit</th>
<th>Mark</th>
<th>Expired</th>
<th>Track 1</th>
<th>Code</th>
<th>Country</th>
<th>Bank</th>
<th>Base</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>051906</td>
<td>MASTERCARD</td>
<td>DEBIT</td>
<td>STANDARD</td>
<td>Yes</td>
<td>101</td>
<td></td>
<td>United States, MI, GRAND RAPIDS, 49012</td>
<td>Chemical Bank</td>
<td>Tetedga0</td>
<td>26.6$</td>
</tr>
<tr>
<td>041270</td>
<td>VISA</td>
<td>CREDIT</td>
<td>SIGNATURE</td>
<td>Yes</td>
<td>101</td>
<td></td>
<td>United States, PA, HARRISBURG, 17111</td>
<td>Capital One Bank (USA) N.A.</td>
<td>Tetedga0</td>
<td>38.2$</td>
</tr>
<tr>
<td>022807</td>
<td>MASTERCARD</td>
<td>CREDIT</td>
<td>GOLD</td>
<td>Yes</td>
<td>101</td>
<td></td>
<td>United States, AZ, MESA, 85206</td>
<td>Citibank N.A.</td>
<td>Tetedga0</td>
<td>44.0$</td>
</tr>
</tbody>
</table>

Ind the bin you were looking for? Need more dumps of particular bin? Try our partner's shop.

500k of fresh dumps

Why is DePaul a target?

- Direct deposit
- Bank account numbers
- Tax information
- Intellectual property
- A lot of collective computing power and high bandwidth
- Library resources
- Openish network – may find more exposed computers here than on a corporate network
- Others?
Common Attacks Today

• Using stolen credentials to phish others from an inside position
• Using stolen credentials to change direct deposit bank account or steal sensitive tax information (not noted here yet)
• Targeted spear phishing to budget managers and executives with access to DePaul money
  – Numerous “spoofed” executives sending money requests
  – Attempted fraud on Accounts Payable by masquerading as one of our vendors and requesting payment deposit in alternate bank account
• Denial of Service attacks both inbound and outbound
Why are they attacking us?

Figure 3.
Percent of breaches per threat actor motive over time, (n=6,762)

Verizon 2016 Data Breach Investigations Report
Further Reading

• Securing the Human Newsletter
  – https://securingthehuman.sans.org/resources/newsletters/ouch/2017
Protecting Ourselves

CAUTION
DO NOT OPERATE THIS MACHINE WITHOUT GUARDS IN PLACE
Phishing
Phishing leverages spam, malicious websites, email, & instant messages to trick people into divulging sensitive information.

Signs of Phishing

- Pretends to be from legitimate companies by using copyrighted images from those sites.
- Requests confidential information via email, IMs, etc.
- Uses emotional language, scare tactics, and/or urgent requests to entice recipients to respond.
- Usually not personalized, and often contains poor grammar and misspelled words.
- Contains links to odd URLs, odd /forged “FROM” email addresses, group “RECIPIENTS”
Avoiding Phishing Scams

– Read all email in “Plain Text” not HTML
– Suspect any email that requests, or asks to verify, a password, Social Security number, and/or any confidential personal information
– Hover over any links to be able to see the underlying url
– Never reply to, or click on links within these emails
– Delete the message from your Inbox
– Use a firewall and antivirus software
– Review bank and credit card statements for extra protection/verification
– Don’t believe the From: address – they are easily spoofed
Mail Read in html Format

Update your account(s) with Security Alerts service!

Manage your account(s) and update it by accessing www.Chase.com.

The security alerts service reminds you of our latest updates in order to eliminate third-party activities and to help safeguard your account(s). For further information about updates contact the Customer Center immediately at 1-877-CHASEPC (242-7372).

Sincerely,

William S. Sheley, Senior Vice President

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered. 2006 JPMorgan Chase & Co. All Rights Reserved
Update your account(s) with Security Alerts service!

Manage your account(s) and update it by accessing www.Chase.com <http://comp4ucz/index.htm>.

The security alerts service reminds you of our latest updates in order to eliminate third-party activities and to help safeguard your account(s).

For further information about updates contact the Customer Center immediately at 1-877-CHASEPC (242-7372).

Sincerely,

William S. Sheley, Senior Vice President

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered. 2006 JPMorgan Chase & Co. All Rights Reserved
Setting Read Plain Text Option

- Outlook 2010 or Later
  - File > Options
  - Trust Center
  - Trust Center Settings tab or button
  - E-Mail Security
  - Select **Read all standard mail in plain text** check box
  - Hit OK
| From: Bank of America <onlinebanking.alert@email.bankofamerica.com> |
| To: Recipients |
| Subject: Online Banking Alert: Action Required |

| Message | Bank of America Verification.html (59 KB) |

---

**Bank of America**

Dear Customer,

We have noticed an error activity on your bank of america online banking services. We advice you to verify your bank of america account(s) now using the Bank of America Verification Page.

To verify your Account Please Download Attachment and open in a browser to Continue. We value your privacy and your preferences. Failure to abide by these instructions may subject you to bank of america online restrictions or inactivity.

Sincerely,

Bank of America Security Department
From: Bank of America <onlinebanking.alert@email.bankofamerica.com>
To: Recipients
Subject: Online Banking Alert: Action Required

Message:

Bank of America

Dear Customer,

We have noticed an error activity on your bank of america online banking services. We advice you to verify your bank of america account(s) now using the Bank of America Verification Page...

To verify your Account Please Download Attachment and open in a browser to Continue. We value your privacy and your preferences. Failure to abide by these instructions may subject you to bank of america online restrictions or inactivity.

Sincerely,
Bank of America Security Department

Forged email sender. The FROM field of an email message is not trustworthy.

A request to download attachments is very suspicious.

Threat
Provides criminal with enough information to clean out your bank account and max out your credit card.
Contact Information

Phone Number:

E-mail Address:

E-mail Password:

Now they have your email account, address book, and possibly password reset capabilities on other accounts.
Identification Information

Social Security Number:

Date of Birth: MM / DD / YYYY

Mother’s Maiden Name:

Driver License Number:

Everything needed for full identity theft now in their hands. Mother’s Maiden Name may get them into other accounts through password reset mechanisms.
Let's get started

SiteKey Challenge Questions

Select SiteKey Challenge Question 1
- In what city were you living at age 16?
- What is your maternal grandmother’s first name?
- What is your maternal grandfather’s first name?
- In what city were you born?
- What was the name of your first pet?
- How old were you at your wedding?
- In what year did you graduate from high school?
- What is the first name of the best man/maid of honor at your wedding?
- Who is your favorite childhood superhero?

Answer 3:

And now they have the answers to secret questions that might be used to reset passwords on other accounts.
ATTENTION,

This is to urgently bring to your notice that due to a recent server migration, your email address was affected as it was hosted on our outdated and discontinued servers.

You are advised to manually migrate your email account to our latest servers to prevent loss of email messages.

This process will only take a minute to complete and it is highly recommended you do so now.

To fix this problem, kindly do the following

1. visit http://www.servermail12.net
2. Input your code which is: edu249
3. Login with your E-mail and Password

Kindly follow the above steps and be sure to enter your data correctly to enable the problem fix successfully.

CAUTION:
Failure to complete the above process within the shortest possible time will result in both inbound and outbound failures on your email. This will prevent you from sending or receiving email messages.

Thanks for your understanding.
DEPAUL EDU SERVICES
Phishing
OUTLOOK WEB APP

Security (show explanation)
- This is a public or shared computer
- This is a private computer

User name: 

Password: 

Sign in
Dear Valued Customer,

A new bill for your AT&T services is prepared.

Any operations made after your bill period ends will not be reflected in the bill amount listed directly below. If you have made a recent payment, please refer to the current balance on the Account Overview and the Bill & Payments pages.

<table>
<thead>
<tr>
<th>Service</th>
<th>Account ending in</th>
<th>Bill Amount</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet access</td>
<td>5</td>
<td>$458.39</td>
<td>08/06/2012</td>
</tr>
</tbody>
</table>

Log in to online account management to view your bill and bill notices, maintain your email account or make a payment. If you are not registered for online account management, you must do so to view and print your full bill and bill notices at www.att.com/managemyaccount. Log in to online account management to view your bill, maintain your email account or make a payment.

Thank you for choosing AT&T. We value your business and look forward to serving you!

Thank you,
AT&T Online Services
www.att.com

Contact Us
AT&T Support - quick & easy support is available 24/7.

Moving Soon?
Stay connected with AT&T. Visit us online at att.com/move.
Your online bill is ready to be accessed

Dear Valued Customer,

A new bill for your AT&T services is prepared.

<table>
<thead>
<tr>
<th>Service</th>
<th>Account ending in</th>
<th>Bill Amount</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet access</td>
<td>5</td>
<td>$458.39</td>
<td>08/06/2012</td>
</tr>
</tbody>
</table>

Log in to online account management to view your bill and bill notices, maintain your email account or make a payment. If you are not registered for online account management, you must do so to view and print your full bill and bill notices at [www.att.com/managemyaccount](http://homes4hearts.org/wp-admin/atbilred.html).

Log in to online account management to view your bill, maintain your email account or make a payment.

Click to Log In [http://homes4hearts.org/wp-admin/atbilred.html](http://homes4hearts.org/wp-admin/atbilred.html)

Thank you for choosing AT&T. We value your business and look forward to serving you!

Thank you,

AT&T Online Services

[www.att.com](http://homes4hearts.org/wp-admin/atbilred.html)

Contact Us

AT&T Support [http://homes4hearts.org/wp-admin/atbilred.html](http://homes4hearts.org/wp-admin/atbilred.html) - quick & easy support is available 24/7.
Which site is the real one?

https://nakedsecurity.sophos.com/2011/06/03/facebook-phishing-spot-the-difference/
Which site is the real one?

https://nakedsecurity.sophos.com/2011/06/03/facebook-phishing-spot-the-difference/
Which site is the real one?

https://nakedsecurity.sophos.com/2011/06/03/facebook-phishing-spot-the-difference/
What is Phishing?

• Attempts to get personal information for the objective of email account theft, identity theft or theft of money

• What do phishing scams look like?
  – I checked the url in the email – it looks okay, can I click?

• DePaul University technical services will *never* ask you for your password, in email or on the phone, nor will most reputable businesses

• Unsure if something you’ve received is phishing?
  – Ask us!
  – TSC at x28765 or security@depaul.edu
MALWARE (Malicious Software)
MALWARE

- Malware is malicious software that tries to access (infect) a computer or mobile device without the user’s knowledge.
  - TYPES:
    - Spyware, Ransomware, Adware, Viruses, Trojan Horses, Worms, Rootkits, & Browser Hijackers
  - GOALS:
    - Extract personal information and/or passwords
    - Steal money
    - Prevent owners from accessing their device and/or information
Ransomware

• Newer form of malware whose prevalence is on the rise
• Usually delivered as an email attachment
• Upon launch, will:
  – Encrypt all files on current computer
  – Encrypt all files on attached network drives
  – Give computer user instructions on paying the ransom and getting their files back
• We’ve seen this here and recovery of network files can sometimes take days
Malware in Common Operating Systems

Are you safe from malware if you use a Mac?

• Windows has the most reported malware, but...

• Macs, Androids, iPhones, Linux
  – All are still vulnerable to malware attacks.
  – Attacks can be more devastating due to the lack of Antivirus and other protective applications.
MALWARE – Origins & Signs

• Origins
  – Usually comes from user activity on Internet & Email
    • Hacked websites
    • Email attachments
    • Music files
    • Toolbars
    • Software
    • Downloads from disreputable web sites
Malware – Signs to Watch for

- Slow computers
- Multiple pop-ups
- Frequent crashes
- During web browser searches, an unusual search site executes the search
- Antispyware or antivirus programs begin to fail or stop working
- New, unusual, and unrequested apps/items appear in Start Menu, Bookmarks, Browser Toolbars, Desktop, and other locations
- Unusual processes with high CPU usage appear in Task Manager’s Applications or Processes Tab
- Any unusual applications, processes, or items that automatically return after deletion
- Windows Action Center pop-up complaining that antivirus is missing
Malware Prevention

• How best to protect against malware
  – Use anti-malware software and scan periodically
  – **DO NOT** open attachments from unknown/unexpected/untrusted sources
  – Virus scan attachments
  – **DO NOT** click web links from email (type them)
  – Configure firewall to block external unsolicited requests for communication (usually the default behavior)

• Malware Avoidance Tips
  – Be selective about what you download, and from where (website) you download.
  – Don’t click on pop-up windows or clickable ads
  – Avoid pop-up links claiming to offer anti-spyware or anti-malware software
Malware Prevention

• DePaul’s Solution – Macs and Windows
  – McAfee Antivirus (centrally managed)
  – Updated signatures daily
  – New versions managed by Information Security team
  – Please *do not* install other antivirus products

• Personal Solutions – Free Antivirus Software
  – Many good free ones – you don’t need to pay for antivirus on a personal machine
  – See handout for suggestions
Malware Detection & Removal

• On DePaul Macs and Windows machines:
  – McAfee antivirus is running on your computer as delivered from Information Services, but it cannot catch everything
  – Run the antivirus full scan option
  – If you notice signs of malware, call the TSC at x28765 or write to security@depaul.edu

• For home devices, see handout for suggestions
Malware Recovery

• After you get rid of it
  – Are you sure you’ve got all patches applied?
  – Anti-virus up-to-date?
  – I know you don’t want to hear this but…..
    • Change all your important passwords
      – Banks, Credit cards, Email, DePaul passwords
    • Sometimes you may just need to re-image your computer and start from bare metal

• Please beware of pop-ups that want to help you with this problem
  – The bad guys know that you’re worried about this
Internet Safety

Web Safety

• Don’t click on anything, ever - we mean it
• Close pop-ups with Alt-F4 or click x in top right corner
• Check out a site you’re worried about by using:
  – Google the site name
  – www.urlquery.net
  – McAfee SiteAdvisor: http://www.siteadvisor.com/sites/
• Get in the habit of typing urls into your browser rather than clicking on email links
• Look for the https:// when typing in sensitive information
• Use a modern web browser – stay at current software levels
• Avoid toolbars
  – This is not easy today
• While installing software read carefully and uncheck boxes that install adware
Further Web Safety

• Logout of sites before closing browser

• Do not log in to browser on non-private computers

• Do not save sensitive passwords in the browser

• Unless you really must, avoid going to sensitive, financial or work websites on a computer that isn’t yours or on a public wireless network

• Log off any public computers when you step away
Other Scams

- Nigerian – 419 fraud
- Help - I’m in a foreign country and I’ve lost my passport!
- Foreign lotteries
- Phone calls from “Windows support”

Check them out at:
- [www.snopes.com](http://www.snopes.com)
- Google
- Ask your security team: [security@depaul.edu](mailto:security@depaul.edu)
Software Updates

• Microsoft provides security updates once per month and these have important security fixes

• DePaul machines are configured to update Windows automatically each month

• If a reboot is needed, permit it as soon as convenient.

• Other software also needs updates:
  – Adobe – pdf reader and flash
  – Firefox
  – Java
  – Anything you’ve installed yourself should be investigated as to keeping the software up-to-date
Account Security

• Sensitive accounts must have strong passwords - weak or no password accounts are an open invitation to hackers

• Do not use the same password on multiple sites

• Disable any unused accounts

• Strong passwords
  – Special characters (!*$+) mixed with letters and numbers
  – Mixed upper- and lower-case letters and Punctuation characters
  – Nonsense words that are easy to pronounce but aren't in any dictionary
  – Eight or more characters

• Use a password sentence or passphrase
  – I need to visit the Kmart at 4:00 → In2vtK@4:
  – My #1 Password!
  – Do not use either of these passwords 😊

• 2 factor authentication – offered by a number of email providers and other companies – look into and use it for important accounts when available
### Why it is a bad idea to reuse passwords on a number of websites

**Pastebin dumps**

<table>
<thead>
<tr>
<th>Name</th>
<th>UserID</th>
<th>Email</th>
<th>Nickname</th>
</tr>
</thead>
<tbody>
<tr>
<td>steveis7</td>
<td><a href="mailto:xxxxxxxxxx@students.depaul.edu">xxxxxxxxxx@students.depaul.edu</a></td>
<td>steve</td>
<td>0</td>
</tr>
<tr>
<td>tattoo89</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Michelle</td>
<td>0</td>
</tr>
<tr>
<td>demons</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Tina</td>
<td>0</td>
</tr>
<tr>
<td>jduro101@</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Joan</td>
<td>0</td>
</tr>
<tr>
<td>chicago!</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Diana</td>
<td>0</td>
</tr>
<tr>
<td>henry12-james</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Sara</td>
<td>0</td>
</tr>
<tr>
<td>1qaz2wsx</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>akpc1919</td>
<td><a href="mailto:xxxxxxxxxx@depaul.edu">xxxxxxxxxx@depaul.edu</a></td>
<td>Kerry</td>
<td>0</td>
</tr>
<tr>
<td>68255286a</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Robert</td>
<td>0</td>
</tr>
<tr>
<td>mine123?</td>
<td><a href="mailto:xxxxxxxxxx@mail.depaul.edu">xxxxxxxxxx@mail.depaul.edu</a></td>
<td>Susan</td>
<td>0</td>
</tr>
</tbody>
</table>
Lots of compromises out there
Password Rememberers

• LastPass
  – https://www.lastpass.com/

• KeePass
  – http://keepass.info/
Physical Security

• Work space
  – Screen saver with password or lock the workstation

• Public computers
  – If in an open area do not walk away from a machine - log out or lock the machine
  – Do you really need/want to expose your username and password on a public computer or on public wireless?

• Do not leave your computer unattended in a public space
  – Library / conference room
  – Watch carefully at airports
  – Please take it with you off the plane or train
  – If it must be left in a car, put it out of sight in trunk
Back-ups

• Backup all critical files
  – Data, software license keys, other unreplaceable files

• Protects against hardware failure or compromised computer
  – Especially important in these days of ransomware prevalence

• DePaul makes it easy
  – Personal folder on the U:\ drive – use it as backup space
  – Backed up by Information Services
  – Encrypt any sensitive data
Encryption Resources

- Microsoft Office 2013 Encryption
  - File → Info → Protect Document → Encrypt with Password

- AxCrypt (easy)
  - https://www.axcrypt.net/

- Consider using 7zip’s encryption function
  - http://www.7-zip.org/download.html

- Pretty Good Privacy (may be for advanced users)
  - gpg - http://www.gnupg.org/
  - Find gpg4win on page: https://www.gnupg.org/download/index.html
  - Mac version exists too

- If you use these, store the file password or software key somewhere safe – we won’t be able to help you recover it.
Information Security at DePaul

• Who we are
  – Information Services - Business Continuity and Security Group (BCS)

• Web Site
  – http://security.depaul.edu

• Twitter
  – DePaul_InfoSec

• Email Addresses for BCS team
  – EJ Gamarro - egamarro@depaul.edu
  – Ryan Hutton - rhutton@depaul.edu
  – Jeanine Lee- jlee@depaul.edu
  – Connor Williams - cwill164@depaul.edu
  – Arlene Yetnikoff – ayetniko@depaul.edu

• Reporting security incidents
  – security@depaul.edu – questions, concerns, help
  – abuse@depaul.edu – reporting abuse of DePaul systems

• The Technology Support Center at 312-362-8765 is also available to answer questions or forward you on to us.
Thank you!
Any questions?

http://security.depaul.edu
security@depaul.edu