HAPPY #CYBERAWARE MONTH

STAYSAFEONLINE.ORG/NCSAM

National Cyber Security Awareness Month

STOP | THINK | CONNECT
Phishing

Two-Step Authentication

LastPass
Phishing

A scam in which criminals contact you in an attempt to harm your computer and/or collect your private information.
How to Identify Phishing

• Bad spelling, poor grammar, or formatting mistakes
• “Urgent action” and threats
• From someone you’ve never met or spoken to before
• Asks for personal details
• May contain graphics or web addresses that look legitimate
Penn Law Staff Meeting Notification

You have a staff meeting email notification.

Click Here to view message.

Thank you
University of Pennsylvania Law School

iraq99.com/wp-content/cache/mail.law.upenn.edu/mail.law.upenn.edu.htm

Penn Law Important UPDATE

You have an important update from UMHS. Click here to Update.

Thank you for using Penn Law Outlook.

comillus.fr/plugins/cart/mail.law.upenn.edu/mail.law.upenn.edu.htm
From: FedEx Standard Overnight <roger.benson@sognefjordhotel.no>
Sent: Sunday, September 18, 2016 11:18:06 AM
To: [redacted]
Subject: Delivery Notification, ID 00384358
Dear Customer,

This is to confirm that one or more of your parcels has been shipped. Shipment Label is attached to this email.

Yours truly,
Roger Benson,
Delivery Manager.
Dear User,

Your account profile will expire today.

Kindly Click Here to validate.

Sincerely,
University of Pennsylvania: Penn

All rights reserved. Copyright © University of Pennsylvania: Penn
From: dave@ffmpeg2lib.com
Date: September 26, 2016 at 11:35:07 PM EDT
To: [redacted]@law.upenn.edu
Subject: Twitter for Edu Law community

Hi Professor [redacted],

My name is Dave and I am an undergraduate student at Columbia. I am trying to establish a list of members of US law schools who are also on Twitter. During my research, I have found that your twitter handle is @

If it is the case, you don't have to do anything. Else, please reply to this email with the correct Twitter handle. Thank you for your time.

Best regards,

Dave.
664511b10ede4e9436dc837bb088f93e
Penn WebLogin

Enter your credentials to initiate a 10-hour Penn WebLogin session.

The session provides single sign-on access to many protected University web resources.

- PennKey
- Password
- Date of Birth
- SSN

Log in
About Penn WebLogin
Subject: URGENT: IMPORTANT NOTICE
Date: Fri, 31 May 2013 08:28:33 -0400
From: Admin University of Pennsylvania <admin_upenn@upenn.edu>
or
From: Admin University of Pennsylvania <hgeltzer@stern.nyu.edu>

Dear,

The management of University of Pennsylvania have mandated that all staffs and students should register for Spam Arrest to help control spam emails sent to our Mail Server.

Register Now for FREE! by Downloading the attached Spam Arrest Page and login with your University of Pennsylvania e-mail details.

This is mandatory to help improve our email services, do not ignore this message.

Thank you for your understanding!

Best Regards,
Management of University of Pennsylvania

This email and any files transmitted with it are confidential and contain privileged information and are intended only for the individual named.
If you received this email by mistake please delete it from your system and notify the sender immediately. You are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. University of Pennsylvania does guarantee that this material is free from viruses or any other defects although due care has been taken to cater for that.
From:
Organization: jagabay@slt.net.lk
Date: Wednesday, September 7, 2016 at 10:31 AM
Subject: Penn Law Important UPDATE

You have an important update from UMHS. Click here to Update.

Thank you for using Penn Law Outlook.
Check out more phishing attempts!

Phishing E-Mail Messages Seen at Penn

The following are samples of confirmed bogus email messages targeting Penn services, or posing particularly large risk. You should never reply, click on links, or provide sensitive personal information in response to these messages.

If you receive a phishing email that is specific to Penn, please forward it to security@isc.upenn.edu.

A list of malicious reply-to and sender address is maintained here.

<table>
<thead>
<tr>
<th>Date</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-21</td>
<td>Profile 21/09/2016 01:10:10</td>
</tr>
<tr>
<td>2016-09-15</td>
<td>Notice! Notice! !Notice!</td>
</tr>
<tr>
<td>2016-09-13</td>
<td>FW, IT-Service Password Update</td>
</tr>
<tr>
<td>2016-09-12</td>
<td>Email Account Activation</td>
</tr>
<tr>
<td>2016-09-09</td>
<td>Email Alert</td>
</tr>
<tr>
<td>2016-08-25</td>
<td>Re: Update</td>
</tr>
<tr>
<td>2016-08-19</td>
<td>Register your Penn Net ID</td>
</tr>
<tr>
<td>2016-08-16</td>
<td>Re: Update</td>
</tr>
<tr>
<td>2016-08-12</td>
<td>Re: Very Important</td>
</tr>
<tr>
<td>2016-08-08</td>
<td>Alert</td>
</tr>
<tr>
<td>2016-08-02</td>
<td>Your membership with Office365 (action required)</td>
</tr>
<tr>
<td>2016-07-29</td>
<td>Notice, Important Document Available</td>
</tr>
<tr>
<td>2016-07-18</td>
<td>Message from Payroll Department</td>
</tr>
<tr>
<td>2016-07-13</td>
<td>Re: Invoice</td>
</tr>
<tr>
<td>2016-06-26</td>
<td>Instructing to you</td>
</tr>
<tr>
<td>2016-04-29</td>
<td>You have 48 pending messages</td>
</tr>
<tr>
<td>2016-04-27</td>
<td>must read</td>
</tr>
</tbody>
</table>
When in doubt, call ITS!

• Email itshelp@law.upenn.edu or call ITS at 215.898.9140 if you receive a suspicious email or you think your information has been compromised.

• Contact us right away; the sooner the better!
Questions about Phishing?

Why great care and consideration should be taken when selecting the proper password.
How can I further protect my data?
Two-Step (Multifactor) Authentication!

• Sign in with your regular password.
• Then enter a secure, unique code sent to you via smartphone app or text.
• Cybercriminals may steal your password, but your account will still be secure.
How to Log in with PennKey Two-Step

First log in using your PennKey and PennKey password as you normally would.
How to Log in with PennKey Two-Step

Then enter a secure, unique code sent via smartphone app.
• Works for all log-on pages that use PennKey and PennKey password

• Not for pages that use LawKey and LawKey passwords
Search for Other Two-Factor Services

Two Factor Auth (2FA)

List of websites and whether or not they support 2FA. Add your own favorite site by submitting a pull request on the GitHub repo.

Search websites

Categories:
- Backup and Sync
- Banking
- Cloud Computing
- Communication
- Cryptocurrencies
- Developer
- Domains
- Education
- Email
- Entertainment
Questions about Two-Step Authentication?
LastPass

How does LastPass Work?
University of Pennsylvania has partnered with LastPass to bring you LastPass Premium!

LastPass is a secure password manager that remembers your passwords so you don't have to. And with LastPass Premium, you can enjoy everything LastPass has to offer, including unlimited sync across all your devices so you always have your passwords with you.

Please enter your University of Pennsylvania email address: *

email@upenn.edu

Do you already have a personal LastPass account that you would like to upgrade to Premium? *

- Yes, I already have a LastPass account that I would like to upgrade.
- No, I do not have a LastPass account but I would like to create one.

* Required
Master Password

• **Master passwords cannot be reset if you forget it!**
• You can only choose to enter a password reminder that will be sent to your email in the event that you forget your master password.

• From LastPass:
• “It is critical that you never forget your new LastPass password. To protect your privacy and keep your data confidential, we do not know what your LastPass master password is. We also do not keep a copy or backup of it.”
YOUR VAULT & ENCRYPTION

See all your accounts and passwords in one easy-to-use "vault." LastPass syncs automatically, so you're always up-to-date. Sensitive data is only encrypted and decrypted locally, with your key, which is never shared with LastPass. 256-bit AES encryption, one-way salted hashes, and PBKDF2 iterations ensure complete security with the power of syncing through the cloud.
AUTOFILL

Because LastPass remembers and fills in all of your usernames and passwords for you, you can finally use a strong, unique password for each online account. LastPass does the work for you.

USER: ........................ ........................
PASS: ........................ ........................
Penn WebLogin

Log in to gain access to many protected University web resources.

**PennKey**

**Username**: agarrett

**Password**: *******

Forgot PennKey **username** / **password**?

[About Penn WebLogin]

[Log in]
For More Information About LastPass

- Penn Law ITS LastPass webpage
- LastPass support website
- LastPass YouTube video tutorials
Have I Been Pwned?

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

142
2
1,444,567,928
2
39,918
2
31,164,417
2

Top 10 breaches

myspace: 359,420,698 MySpace accounts
LinkedIn: 164,611,595 LinkedIn accounts
Adobe: 152,445,165 Adobe accounts
Badoo: 112,005,531 Badoo accounts
VK: 93,338,602 VK accounts
Dropbox: 68,648,009 Dropbox accounts
tumblr: 65,469,298 tumblr accounts
iMesh: 49,467,477 iMesh accounts
Fling: 40,767,652 Fling accounts
Last.fm: 37,217,682 Last.fm accounts

Sensitive breach, not publicly searchable
Unverified breach, may be fabricated

View all breaches
Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned  Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords
Cybersecurity To Do

1. **Sign up for PennKey Two Factor Authentication.**

2. **Set up your LastPass Premium account.**

3. Reset passwords on compromised accounts, and sign up for email alerts from **Have I Been Pwned?**

4. **Secure other accounts with two-factor authentication.**
Questions?

Password entropy is rarely relevant. The real modern danger is password reuse.

How so?

Password too weak.

Set up a web service to do something simple, like image hosting or tweet syndication, so a few million people set up free accounts.

BAM, you've got a few million emails, default usernames, and passwords.

Tons of people use one password, strong or not, for most accounts.

Use the list and some proxies to try automated logins to the 20 or 30 most popular sites, plus banks and PayPal and such.

You've now got a few hundred thousand real identities on a few dozen services, and nobody suspects a thing.

And then what?