ITS Lunch & Learn

Dan Darrow: ddarrow@law.upenn.edu
Christine Droesser: cdroesse@law.upenn.edu
Amelia Garrett: agarrett@law.upenn.edu

1. HALLOWEEN
2. PUMPKIN SPICE LATTES
3. NATIONAL CYBERSECURITY AWARENESS MONTH

#BeCyberSmart
Cybersecurity Attitudes & Behaviors National Poll

• **78%** of people consider staying secure online a priority

• **34%** noted they often feel overwhelmed by information and, as a result, minimize their online actions

• **46%** felt frustrated while staying secure online

• **39%** of users trying to keep safe felt information on how to stay secure online is confusing

• Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022
Overview

• Sensitive Data
• Privacy Tips
• Laptop/Mobile Device Security
• Phone/Texting Scams
• Email/Phishing Scams
• Compromised Accounts/Security Incidents
• Password Manager
• To Do's/Key Takeaways
Sensitive Data

See Penn's Data Risk Classification Guide: [https://www.isc.upenn.edu/security/data-classification](https://www.isc.upenn.edu/security/data-classification)

Confidential University Data includes

- **Sensitive Personally Identifiable Information**: Information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to Penn. Examples may include, but are not limited to, Social Security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information Penn has promised to keep confidential, and account passwords or encryption keys used to protect access to confidential University data. Includes student records (FERPA) and employee records.

- **Proprietary Information**: Data, information, or intellectual property in which the University has an exclusive legal interest or ownership right, which, if compromised, could cause significant harm to Penn. Examples may include, but are not limited to, business planning, financial information, trade secrets, copyrighted material, and software, or comparable material from a third party when the University has agreed to keep such material confidential.

- **Other data**: Other data whose disclosure would cause significant harm to Penn or its constituents.
Sensitive Data

Penn Privacy Policies: [http://www.upenn.edu/oacp/privacy/policiesguidance/](http://www.upenn.edu/oacp/privacy/policiesguidance/)

Includes:
• Applicant Data Policy
• Confidentiality of Faculty & Staff Records – HR Policy 201
• Confidentiality of Student Records
• IT Security Policy
• Privacy of Alumni Data
• Social Security Numbers

Lots of Guidance Documents as well:
• Guidance on Disposition of Documents & Data of Faculty/Staff who have Left Penn
• Records Destruction
• Responding to Requests for Lists of Student/Faculty/Staff Information
Protecting Data

• Be mindful of the data you are responsible for, its sensitivity, where the data is stored, and if it is shared with others.
• Delete or redact what is not needed. Redact SSNs if required to keep documents. Retention Guide: https://archives.upenn.edu/records-center/resources/retention-schedules

Store Sensitive Data Responsibly
• SharePoint Secure Sites
• Do not store Law School data on your personal/home computers
• Do not store/share via USB Keys
• Share via SecureShare or other sanctioned tools (not email)
Data Privacy Tips

Limit the amount of personal information that you share online by reviewing/updating your privacy settings on websites, apps, and mobile devices at least one or two times per year.

*Not sure where to begin?*

The National Cyber Security Alliance (NCSA) website ([https://staysafeonline.org/resources/manage-your-privacy-settings/](https://staysafeonline.org/resources/manage-your-privacy-settings/)) provides direct links to manage your privacy settings on popular devices and online services including Google, Facebook, Amazon, Instagram, web browsers, etc.
Data Privacy Tips

- Turn on **two-step verification** or multifactor authentication (MFA) whenever it's offered (100% required for online banking).

- Use **incognito or private web browsing** windows to limit the information collected in your browsing history, cookies, or online forms.

- **Online quizzes** and games can be fun but think about how the personal details from your social media profiles might be sold to or shared with data collection companies.

- **Delete apps** you don't use.

- **Keep apps up to date**.

- **Don't overshare**! Limit the kinds of personal information you share on social networking sites.
Social Media: Consensual Doxxing

Matching accounts across social media platforms is easier than you’d expect.

You’re only as secure as your least secure friend or family member.
Chat GPT & AI Privacy

• There are no expectations/agreements for data privacy and security. Data entered into ChatGPT and other AI tools should not be considered private.

• Users should not put confidential/sensitive information into the system including FERPA, PHI/HIPAA, financial or other regulated data.

• More information [https://www.law.upenn.edu/its/docs/chat-gpt/](https://www.law.upenn.edu/its/docs/chat-gpt/)
47% of American adults have had their personal information exposed by cyber criminals.

From: https://www.cisa.gov/be-cyber-smart/facts#note_microsoft-consumer-reports
Recommendations & Best Practices for Laptops and Mobile Devices

• Our security recommendations - How can you stay secure?
  • Keep your software up to date
  • Only use supported software/tools
  • Run anti-virus/anti-malware software on every device
  • Practice good web browsing habits and use a VPN
  • Ask questions and report suspicious behavior ASAP!

• Preparing for the worst – What to do if your device is lost/stolen.
Update Your Software

• Don’t wait -> Update!
• Turn on automatic updates for all personal devices.
• Law-managed devices have automatic updates enabled by default.
Update Notifications - Browsers

Microsoft Edge

Google Chrome
Update Notifications - Misc.

- Microsoft Office
- Adobe Acrobat
- GlobalProtect VPN
1 in 3 homes with computers are infected with malicious software.

Source: https://www.cisa.gov/be-cyber-smart/facts#note_aarp
Use Supported Software

• ITS supports and licenses a wide variety of software to meet your individual and departmental needs.

• Have software questions? Ask us!
Anti-Virus & Anti-Malware

• Keeps you proactively safe from well-known attacks.
  • This is done through virus signatures & definitions.

• All Law-managed devices run an advanced version of Microsoft Defender.
  • Scans can be run at any time from the Windows Security application.

• Penn offers Sophos Home for personal devices.
  • All Faculty, Staff, and Students are eligible to download/install!
Web Browsing - VPN

• One of the most vulnerable attack vectors!
  • Many apps today are “browser-based”
  • Public wifi is not to be trusted
    • Bad actors can “spoof” common public network names (e.g. “Google Starbucks”)

• Your personal info has real value and should always be protected.
  • Use GlobalProtect VPN.
The University offers an enterprise VPN service called *GlobalProtect* available to the Penn community.

Virtual Private Networking (VPN) software creates an encrypted connection between your off-campus computer/device and Penn’s network. Penn faculty, staff and students can use the GlobalProtect VPN to connect securely to the campus network and access restricted services from off-campus.

More Info: [https://www.law.upenn.edu/its/docs/remote/vpn-globalprotect.php](https://www.law.upenn.edu/its/docs/remote/vpn-globalprotect.php)
Alongside being careful online, you should also use a modern and secure web browser.

**ITS recommends Microsoft Edge as your default browser.**

**Why Edge?**
- Saves all general and privacy settings to your LawKey account - syncs across devices.
- Built-in SmartScreen detects malicious webpages, prevents access & file downloads from harmful sites.
- Tracking prevention enabled by default.
Fake Browser Pop-ups/Notifications

• How to spot a fake:
  • Spelling/grammar errors.
  • Bad quality logos/images.
  • Does the URL look weird?
  • Are you even using the software shown in the notification?
Fake Browser Pop-ups/Notifications

• Clear browsing data to remediate (especially site data and permissions).
  • Instructions: Edge | Chrome
Missing/Stolen Devices

• As soon as you realize your laptop or personal device used to access law resources is missing or has been stolen:
  • **Contact ITS ASAP!**
    • We will work with you to reset your account passwords and assess the impact.

• To be extra safe, Apple and Google offer tools to remotely lock and erase your mobile device if needed.
  • Apple’s “Find My” app or [icloud.com/find](http://icloud.com/find).
  • Google’s “Find My Device” app or [android.com/find](http://android.com/find).
Spot that Spam!
Phone Call & Text Scams

• The call is **unexpected. Urgent action** is needed.
• The caller claims to be from a government agency, a vendor (e.g. Microsoft), a financial institution, your insurance company, or some other trusted group.
• Asks for **personal details** (they may already know some personal details).
• They could be **spoofing a legitimate number**.
• Scam attempts happen over text too!
Phone Call & Text Scams

• What you should do:
  • **Hang up** the phone. Don’t provide any information.
  • If you think the call may have been legitimate, find the phone number for the agency/bank/vendor and call that number.
  • Some vendors do not have public customer service phone numbers anymore! You may need to contact them via email.
  • Report the text message as spam on your messaging app.
Common Scam Examples

- Unauthorized transaction on your account
- Fake delivery error/package tracking
- Fake online purchase confirmation
- Your credit/debit card has been deactivated/stolen
- Fake IRS audits, fake bills
- Fake job offer/interview
- Extended warranty and loan scams
- Tech support/device/account compromise
- Extortion, threats of arrest
- Your iPhone/iCloud has been breached
AI-Assisted Voice Mimicry

• AI tools such as Speechify can clone your voice with just a 30 second recording.
• They often ask you to wire money, send cryptocurrency, or buy gift cards.
• Hang up and call the person on a number you know is theirs or contact them through another family member or mutual friend.
Scams Across Multiple Contact Points

• Some scammers will contact you over text, phone call, and email.

• Your contact info is publicly available. Scammers can easily find your phone number and email.
How ITS Enforces Email Security

• We have protocols and certificates to communicate and authenticate with other email servers (e.g. DKIM, SPF, DMARC)

• We employ Microsoft’s powerful spam filtering tools.
The Past Week at Penn Carey Law:

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total email</td>
<td>437,285</td>
<td></td>
</tr>
<tr>
<td>Anti-malware</td>
<td>60</td>
<td>0.01%</td>
</tr>
<tr>
<td>Anti-spoof</td>
<td>3,831</td>
<td>0.88%</td>
</tr>
<tr>
<td>Anti-spam</td>
<td>14,908</td>
<td>3.41%</td>
</tr>
<tr>
<td>Email with no detected threats</td>
<td>328,616</td>
<td>75.15%</td>
</tr>
</tbody>
</table>
Problems with Enforcing Email Policy

• Despite these defenses, malicious messages still get through sometimes.

• Email filtering is a balancing act. Legitimate organizations don’t always employ best practice. If rules are too strict, legitimate emails will be filtered as spam.

• Malicious emails are becoming extremely convincing, both technically and socially.

• Your eyes and emails to ITS are important spam alert tools! You often catch malicious emails earlier than our automated tools!
Spot that Email Spam!

• Some spam emails look very legitimate (spoofing)
• “Urgent action” and threats
• Unexpected / unsolicited
• Asks for personal details
• Don’t recognize the sender
• URL(s) / attachment(s)
• Especially a URL that links to a login page (don’t even click the URL to find out).
From: Law IT Support <andy@shopperswholesale.ca>
Sent: Thursday, April 8, 2021 3:46 PM
To:
Subject: You just have received a Voicemail

Your caller left you a message. Find details below
Caller ID : +1 (408) 253 - 686
Date : 08/04
Duration : 0:56 Sec

Download Attachment Above

Note: this is an automated message and need mediate attention please
Organization : Law.upenn.edu
Account Summary : Support@Law.upenn.edu

1 Attachment

receiptLaw253.htm
  509 Bytes
A secured Voicemail has been shared with you canvashelp@law.upenn.edu for your review

Recordings@law.upenn.edu reported a month ago (Thu, Sep 1 5:12 AM) via Email
To: canvashelp@law.upenn.edu

This sender has been verified from safe senders list.

Download Attachment to view your Voicemail message on Wednesday, August 31, 2022

Hi canvashelp@law.upenn.edu, You have received a new voicemail.

<table>
<thead>
<tr>
<th>From</th>
<th>25146870*** (WIRELESS CALLER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date &amp; Time</td>
<td>Wednesday, August 31, 2022</td>
</tr>
<tr>
<td>Duration</td>
<td>0:46</td>
</tr>
<tr>
<td>In mailbox</td>
<td>112 <a href="mailto:canvashelp@law.upenn.edu">canvashelp@law.upenn.edu</a></td>
</tr>
</tbody>
</table>

WARNING: MAILBOX 112 IS FULL. PLEASE DELETE SOME VOICEMAILS TO ENSURE CONTINUED SERVICE.

** You can always view your voicemail history in the canvashelp

Hide

1 Attachment

wav200canvashelp@law...
3.14 KB
You were found by people
LinkedIn reported 7 months ago (Sat, Feb 26 7:51 AM) via Email
To:itsurgent@law.upenn.edu <itsurgent@law.upenn.edu>

Sender’s email: gzdhy@v150-95-140-177.a085.g.tyo1.static.cn0de.io

You appeared in searches this week
UnitedHealth Group, Time Warner

You were found by people from these companies

Who’s looking?

Never miss an update with LinkedIn app
Download the app

This email was intended for itsurgent (itsurgent@law.upenn.edu).
Learn why we included this.
Hello there!

Unfortunately, there are some bad news for you.

Some time ago your device was infected with my private trojan, R.A.T (Remote Administration Tool), if you want to find out more about it simply use Google.

My trojan allowed me to access your files, accounts and your camera.

I RECORDED YOU (through your camera)

After that I removed my malware to not leave any traces.

If you still doubt my serious intentions, it only takes couple mouse clicks to share the video of you with your friends, relatives, all email contacts, on social networks, the darknet and to publish all your files.

All you need is $1800 USD in Bitcoin (BTC) transfer to my account (Bitcoin equivalent based on exchange rate during your transfer).
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**

About Penn WebLogin

Log in
Pen Law Webmail
Microsoft Office Outlook Web Access

Note: Outlook Web Access requires an Exchange account. ITS offers Exchange accounts to faculty and staff.

Security ( show explanation )

- This is a public or shared computer
- This is a private computer

Use the light version of Outlook Web App

User name: [input]
Password: [input]

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.
Thomas Buchanan shared a file with you

Malware shared from SharePoint

FWD: Facilities Management/Services Victoria Iannotta Sent You This File

ASSESSMENT FILE

This link will work for anyone.

Open
From: Upenn-Portal <upenn.edu>
Sent on: Wednesday, September 13, 2023 3:04:44 PM
To:
Subject: Notification for

You have one important Notification.

Click Here to view Notification details

University of Pennsylvania
You have received a secure message

If you have concerns about the validity of this message, contact the sender directly.
To retrieve your encrypted message, follow these steps:
1. Click the attachment, securedoc.html.
You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser.
2. Enter your password.
Mobile device users: forward this message to mobile@res.cisco.com. You will be emailed a link where you can enter your password and view the secure email message.

CONFIDENTIALITY STATEMENT. The information contained in this e-mail message, including attachments, is the confidential information of, and/or the property of the individual or entity named in the message. If you are not an intended recipient or you received this in error, then any review, printing, copying or distribution is strictly prohibited. If you have received this in error, please notify the sender immediately by reply e-mail.

law.upenn.edu Secure Email Encryption

SecureDoc_EFT_Payment_Completed.html
(8.64 KB)
✓ Incoming Doc
You have received a new pdf file shared with you online

<table>
<thead>
<tr>
<th>Pages</th>
<th>File #327636 Copy DOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received</td>
<td>January 31, 2022</td>
</tr>
<tr>
<td></td>
<td>View File</td>
</tr>
</tbody>
</table>

CONFIDENTIAL AND PRIVILEGED

This email message (including any attachments) contains information that may be confidential, be protected by the attorney-client or other applicable privileges, or constitute non-confidential business information and is intended to be conveyed only to the designated recipient(s). Any unauthorized review, use, disclosure, or distribution is prohibited. If you are not an intended recipient of this message, please notify the sender immediately.

Thank you.
Account Security info

We received an instruction from your mail account requesting for your account termination, please ignore this message if the request was from you.

Your account would be deleted from our system in the next 48 hours.

(Note: All mails in your inbox, spam, draft, and sent items would be terminated, and access to your account would be denied.)

Click on cancel request if the message wasn't from you.

CANCEL REQUEST

Cancel the termination request if you didn't authorize this request and protect your account.

Thanks,
The Account Team

This email is autogenerated. Replies will not be answered
Security Authentication

You are required to update your Multi Factor Authentication security via QR scan today Friday, 28 Sep 2023

Scan the above QR code with your smartphone or tablet camera to update.

Update your MFA within 2 days of receiving this notification.

To avoid any interruption.
Dear User

Your email password will expire today.

Click on the link to keep using your current password.

Keep Current Password

Your account might be locked after 48 hours.

Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA
From: "Support Notification@law.upenn.edu" <Marti@beanangel.org>
Date: April 26, 2023 at 12:40:25 AM GMT+1
To:
Subject: Tuesday, April 25, 2023 Password Reminder Message for

This sender might be impersonating a domain that’s associated with your organization. Learn why this could be dangerous.

Microsoft 365

Password Authentication Service

Hello,

The Password to your email account will be expiring soon,

To keep using your password verify request below,

KEEP MY PASSWORD

⚠️ ACTION REQUIRED TO AVOID EMAIL CLOSURE

©2023 MICROSOFT EXCHANGE
Dear User,

This is to inform you that, as of March 17, 2023, your campus email account will be disabled.

This message is being sent to you because suspicious activity was detected in your email account. It appears that your account was accessed from an unknown location, device, or app, or it may have been linked to multiple other accounts or created by a program that violates Campus policies.

Before you can continue using your Campus Email account, we must verify your identity. To do so, please navigate to the Campus Email System and proceed to the Email Deactivation page. This will allow us to confirm your identity and reinstate your account if appropriate.

If you have any additional questions or require assistance, please visit the Campus Support System FAQ. We apologize for any inconvenience this may cause and thank you for your understanding.

Best regards,

Wellington Adriano
2023 IT Support Services
Office of Information Systems & Technology
5:20

+1 (!

Text Message
Today 5:15 PM

Hi, let me know if you got my text.- Thanks, Theodore W. Ruger

The sender is not in your contact list.

Report Junk
officeofpresidentmail@gmail.com appears similar to someone who previously sent you email, but may not be that person. Learn why this could be a risk

Sheridan,

If it wouldn't be too much trouble, May I request your assistance in dealing with certain administrative expenses that need tending while I attend a conference?

Is there any way that payment can be processed today by mailing out a check or through wire transfer?

In addition, are PayPal or Zelle services available as options for payment? Finally, could you please relay the current account balance at your earliest convenience?

Thanks.
I need you to pick up three $200 eBay gift card for me at the store as I need to make use of them ASAP, I will reimburse you when I’m out of the meeting, when you get them scratch off the silver panel that shows off the claim code and send me a picture of it on here. And don’t forget to keep the hard copies for me.

Thanks!

On Fri, 24 Jan 2020 at 23:05...

Right now? Yes.

From: .law.upenn.edu@gmail.com>
Sent: Friday, January 24, 2020 4:51 PM
To: 
Subject: I want a quick response

Are you free?

--

Executive Director
Hello,

Kindly find the attached revised receipt.
Please Sign Documents

Jessica Price has sent Quote Order Form Renewal No Signature - Q-46658 - Ver. 1.pdf for your signature.

Please review Renewal Order # Q-46658 for Penn Law School (Soon To Be Carey Law School).

Please click on the view document button to review and add PO details. Once complete, you will receive a fully executed copy of the order. Please also provide a physical copy of the PO and let us know if you have any questions.

Please click on the button below to start the signing process.

To reassign the signer, click here
To view the audit trail, click here
Merchant Credit $3560.56 was issued to your account

For safety reasons, please download attachment to review payment. Update and verify your account ownership is required as a means to accept your payment.

Notice: Account will be credited within 24hrs after you verify your ownership

Thank you for choosing American Express

CONFIDENTIALITY STATEMENT. The information contained in this e-mail message, including attachments, is the confidential information of, and/or is the property. The information is intended for use solely by the individual or entity named in the message. If you are not an intended recipient or you received this in error, then any review, printing, copying, or distribution of any such information is prohibited, and please notify the sender immediately by reply e-mail.
From: s_workday@mtm-inc.net
Sent: Tuesday, March 7, 2023 11:43 PM
To: support@checkissuing.com
Cc: achelpdesk@mtm-inc.net
Subject: Remittance Information SUP-109421:Check Issuing,LLC DBA Checkissuing.com

Attached is the Remittance Advice for your payment in the amount of $ 55890.19.

For assistance, please contact your Network Representative.

Thank you.

View Less

Attachments (1)

Invoice-2023012348796490720230123487964907.htm (49.6 KB)
New Invoice Document Received For clinic@law.upenn.edu

Dear clinic,

You have a document from Xerox Scanner.

<table>
<thead>
<tr>
<th>Pages:</th>
<th>2 Full Scanned PDF/HTML File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received:</td>
<td>2023-01-24</td>
</tr>
<tr>
<td>ID:</td>
<td>2625258</td>
</tr>
</tbody>
</table>

Attachments (1)

ATT00001.htm

(0.41 KB)
webmaster,

Our records indicate that the payment method you used to purchase Exchange Online was declined Wednesday, September 20, 2023 9:00 p.m.

See Billing statement To continue using law.upenn.edu.

Sincerely,
Billing Team
Junk Folder

- Check your Junk Folder occasionally to see if something was sent there erroneously.
- Sender could be spoofing law.upenn.edu address.
- Consider all email in Junk Folder spam or phishing unless you are very confident about its legitimacy.
Spam Attack Response Protocol

• Please forward all suspicious emails to itshelp@law.upenn.edu

• ITS will:
  • Assess the size of the attack
  • Send an advisory email if large in scope
  • Block the sender
  • Run backend process to move the email to Junk Folder
Questions about Phishing?
How ITS responds to compromised accounts

• Remove improper access to your account. This includes checking Self Service Pass Password Reset and MFA settings.

• Reset account password to a temporary password.

• Remotely run anti-virus and anti-malware scans.

• Consult with the compromised user, Penn Privacy/Info Security, logs, etc. to determine what information was accessed and for how long.
Everyone gets pwned sometimes

`;--have i been pwned?

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

amelia.e.garrett@gmail.com

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

HAUTELOOK

HauteLook: In mid-2018, the fashion shopping site HauteLook was among a raft of sites that were breached and their data then sold in early-2019. The data included over 28 million unique email addresses alongside names, genders, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords

Poshmark: In mid-2018, social commerce marketplace Poshmark suffered a data breach that exposed 36M user accounts. The compromised data included email addresses, names, usernames, genders, locations and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it be attributed to "in South Florida ever since."
Two-Factor Your Personal Accounts

• Bank
• Financial accounts and Credit Cards
• Banking apps (Venmo, CashApp)
• Social Media
• Personal Email
• Third-party Tax Service
• Government Tax Service (PA myPATH)
• Shopping apps (Amazon)
• Anywhere where payment info is saved
PennKey Self-Service Password Reset

Please set up PennKey SSPR!
Don’t ignore the daily reminder!

https://accounts.pennkey.upenn.edu/pwm/private/updateprofile
Strong Passwords & Password Management

- Only 33% of individuals create unique passwords for every account*
  - Only 18% use a password manager*

- 100s of passwords? =

*Source: The Annual Cybersecurity Attitudes and Behaviors Report (2022)
Passphrase

UNCOMMON (NON-GIBBERISH) BASE WORD

Order unknown

Troub4edor & 3

Caps? Common substitutions Numeral punctuation

(You can add a few more bits to account for the fact that this is only one of a few common formats.)

~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(Plausible attack on a weak remote web service. Yes, cracking a stolen hash is faster, but it is not what the average user should worry about.)

Difficulty to guess: EASY

Was it trombone? No, troubador. And one of the Os was a zero?

And there was some symbol...

Difficulty to remember: HARD

Correct horse battery staple

Four random common words

~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

Difficulty to guess: HARD

That's a battery staple. CORRECT!

Difficulty to remember: You've already memorized it

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Strong Passwords & Password Management

• Our recommendations:
  • Longer is stronger:
    • At least 16 characters is ideal.
    • Great defense against password cracking software.
    • 5-7 word “passphrase” of unrelated words (hard to create, easy to type).
  • Unique:
    • A password should never be used for more than one account.
    • Password manager helps here.
Strong Passwords & Password Management

• Use a password manager:
  • LastPass Premium is available for all members of the Penn community!
  • Sign up link here - https://lastpass.com/partnerpremium/upenn
Other Password Managers

• The University is currently evaluating password managers.
  • You will be able to easily export passwords from LastPass into a new system.
  • LastPass is still recommended.
  • The toughest part is centralizing your credentials!
1. **Always** report suspicious activity and emails to ITS.
2. Be skeptical!
4. Install OS/application updates.
5. Don’t reuse passwords.
6. Use a password manager.
7. Email, phone, and text are all vectors for scams/spam.
Cybersecurity Action Items

1. Set up your LastPass account and ensure you have unique passwords: https://lastpass.com/partnerpremium/upenn


4. Check for compromised accounts, change compromised passwords, sign up for alerts: https://haveibeenpwned.com
Questions?

HARBINGERS of
HUMAN MISERY:
fire, flood, famine, drought...
and CYBER ATTACK

R.I.P.
cause of death: phishing

R.I.P.
cause of death: outdated software

R.I.P.
cause of death: "password123"

Guaranteed to keep CIOs up at night...