Cybersecurity Awareness Training

be vigilant but unafraid!

Leo F. Howell
Chief Information Security Officer
lfhowell@uoregon.edu
University

1. **COMPLIANCE** increases business opportunities; required by:
   a) DFAR, FAR, Data Use Agreements (research)
   b) HIPAA, FERPA, GLBA (financial aid)
   c) GDPR (EU persons)
   d) State Laws (OR, CA, CT, …)

2. **DATA BREACHES** cost money and tarnishes our reputation losses

3. **DENIAL OF SERVICE** disrupts operations

4. **SOCIAL RESPONSIBILITY** extends to Data Protection

YOU

1. **Research** at risk
2. **Bank Account** may be emptied
3. **Medical Records** subject to theft or exposure
4. **Embarrassment** via exposure of private social media interactions
5. **Computers Locked** for ransom
6. **Indictment** without guilt
Meet the adversary...

Script Kiddies

Hacktivists?

Nation States

Insiders

Organized Crimes

Hacktivist?
Common attack methods

- **Phishing**
  - Email - Phishing
  - Phone - Vishing
  - Text - Smishing

- **Hacking**
  - Password theft
  - Backdoors
  - Website exploits

- **Malware**
  - Ransomware
  - Key loggers
  - Spyware
YEAH IF WE COULD JUST STOP CLICKING ON PHISHING EMAILS, THAT'D BE GREAT.
Can you spot the phishing?

1. Fake Domains uoregon.edu
2. Urgency
3. Impersonated / Unknown Sender
4. Unexpected Tone / Request
5. Flattery
6. Letter Substitution
7. Bad Grammar
Dear Dr. [X],

I recently read your article: [Title]. It was very useful in my field of research. I wonder, if possible, to send me these articles to use in my current research:


Thanks for you Cooperation in Advance.
Assoc. Prof. [Name]
Dear Dr. [X],

I recently read your article: [Title]. **It was very useful** in my field of research. I wonder, if possible, to send me these articles to use in my current research:


Thanks **for you Cooperation in Advance.**
Assoc. Prof. [Name]
Dear Dr. [X],

I recently read your article: [Title]. It was very useful in my field of research. I wonder, if possible, to send me these articles to use in my current research:


Thanks for your cooperation in advance.

Assoc. Prof. [Name]

- $3.4B IP Theft
- 3,800 Professors targeted, across
- 144 U.S. universities
- 10 Indictments
- n UO Faculty & Staff Compromised
From: Michael Schill [mailto:markross@emailolympic.org]
Sent: Friday, March 02, 2018 2:02 PM
Subject: Michael Schill as Shared a file with you using One Drive

Hello,

Please find attached the Look Ahead files for Friday March 2nd, 2018

Open

Kindly let me have your opinion

Michael Schill
541-346-3936
President
Phishing-4-whales with…
sender impersonation, bad link, tone

From: Michael Schill [mailto:markross@emailolympic.org]
Sent: Friday, March 02, 2018 2:02 PM
Subject: Michael Schill as Shared a file with you using One Drive

Hello,

Please find attached the Look Ahead files for Friday March 2nd, 2018


Kindly let me have your opinion

Michael Schill
541-346-3936
President
From: bart.novoner@uoregon.com

Hello You,

Please purchase 6 gift cards valued at $250 each and send me the numbers right away. I will tell you a funny story about this when I return to the office, but send me those cards NOW.

Bart
From: bart.novoner@uoregon.com

Hello You,

Please purchase 6 gift cards valued at $250 each and send me the numbers right away. I will tell you a funny story about this when I return to the office, but send me those cards NOW.

Bart
Safari malware…

From: andrea@uoreqon.edu

Hello You,

Must see pictures from my safari tour? http://dropbox.com/andresafari. Don't share, I am embarrassed about a few of them.

Andrea
From: andrea@uoregon.edu

Hello You,

Must see pictures from my safari tour.
http://dropbox.com/andreas_safari. Don't share, I am embarrassed about a few of them.

Andrea
From: ciso@uoregon.edu

Hello Susie,

The Information Security Office has determined that your DuckID may have been compromised.

Please change your password as soon as possible then reply to this email to let us know when you have done so.

To do this faster and more securely, click use this password change tool: https://securePasswordTool.Uoregon.edud.in.

Thank you,
CISO’s Office
From: ciso@uoregon.edu

Hello Susie,

The Information Security Office has determined that your DuckID may have been compromised.

Please change your password as soon as possible then reply to this email to let us know when you have done so.

To do this faster and more securely, click use this password change tool: https://securePasswordTool.uoregon.edud.in.

Thank you,
CISO’s Office
Dumb hacker!

From: Mirian Livia Oliveria <mirian.oliveria@cultra.gov.br>

Your Password have expired [CLICK HERE](http://www.cultra.gov.br) to verify
Dumb phish!

What’s missing?

itsrviceupdate.ulcraft.com
"Unable to display message" phish

From: <obfuscated>@uoregon.edu>
Date: Tuesday, August 28, 2018 at 7:42 AM
To: Information Services <isnews@uoregon.edu>
Subject: Re: Protect your devices from Meltdown and Spectre security vulnerabilities

Unable to display this message

Click here to open this message
Logged out due to inactivity. Sign in to continue
"Unable to display message" phish

27K Users Received the Msg
15K Users Read Msg
62K Msg Deleted by Security
653 Users Compromised/Disabled
15K Users Password Changes
$80K+ in person-hours for Response
Dear Greese,

You are receiving this Important security notification as a member of the university.

You have an important notifications from the University of Oregon. Please review the information below immediately for your security on campus.

OU Security Notification

Sincerely,

University of Oregon
From: University of Oregon <jw13925@my.bristol.ac.uk>
Sent: Wednesday, March 6, 2019 9:57 AM
To: George Reese
Subject: Important Campus Security Notifications

Facebook

Dear Greese

You are receiving this Important security notification as a member of the university.

You have an important notifications from the University of Oregon. Please review the information below immediately for your security on campus.

OU Security Notification

Sincerely,
University of Oregon

Just Wrong!!
Dear Greese,

You are receiving this Important Notice because you have an important notification information below immediately if you are not aware of it. It is a serious matter and requires immediate action.

**OU Security Notification**

Sincerely,

University of Oregon

- ~ 80 users suspected of giving up DuckIDs & passwords and/or 95#s & PACs
- 14 users’ direct deposit accounts and routing numbers changed to the hacker’s
General phishing tips

- Mouse-over before you click
- Fake Domains uoregon.edud
- Flattery
- Urgency
- Unknown sender
- Unexpected tone
- Unusual request
- Letter Substitution
- Bad Grammar

- Follow your gut!
- Ask a colleague if you are unsure
- Don’t trust links and phone numbers in email
- Ask Security by forwarding to phishing@uoregon.edu
Key Message on Phishing

Don't get Phished, Smished, Vished ....

By a....

Dumb Hacker!
Password too long to remember?

GOOD.
# Password game

## Good Ones

<table>
<thead>
<tr>
<th>Password</th>
<th>Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>W@r 15 b@d @1w@y5</td>
<td>Strong (76)</td>
</tr>
<tr>
<td>My 3y3s @r3 p1nk</td>
<td>Strong (70)</td>
</tr>
<tr>
<td>This is my story</td>
<td>Strong (69)</td>
</tr>
<tr>
<td>What is fake news?</td>
<td>Strong (87)</td>
</tr>
<tr>
<td>My secret bucket list item is to sing in public</td>
<td>Very Strong (217)</td>
</tr>
<tr>
<td>I hate math, but I totally dig chemistry</td>
<td>Very Strong (197)</td>
</tr>
</tbody>
</table>

## Bad Ones

- 123456
- Letmein
- Football
- Iloveyou
- Admin
- Welcome
- Monkey
- Abc123
- hello
- Starwars

- Time, 2017
Password Game

Good One OR Bad One

Login Required

Please log in with your Duck ID to access the requested service. To protect your privacy, always log out and quit your web browser when finished.

Username: toddbay
Password: Toddbay$

Login
Password Game

Good One OR Bad One

Login Required

Please log in with your Duck ID to access the requested service.

To protect your privacy, always log out and quit your web browser when finished.

Username: marys Password: Iloveyou!

Login
Password Game

Good One    OR    Bad One

Login Required

Please log in with your Duck ID to access the requested service.
To protect your privacy, always log out and quit your web browser when finished.

Username:    Password:

samanp        TheR@t5atemydinner

Login
Password Game

Good One  OR  Bad One

Login Required

Please log in with your Duck ID to access the requested service.
To protect your privacy, always log out and quit your web browser when finished.

Username: samanp
Password: TheR@t5atemydinner2

Login
Password Game

Good One OR Bad One

Login Required

Please log in with your Duck ID to access the requested service.

To protect your privacy, always log out and quit your web browser when finished.

Username: mandyt
Password: lwillgob@cktoVT

Login
General password tips

- Use *password-phrase* instead
- Use 2-Factor Authentication
- Use 5ub5t1tut10n5
- Use more than 10 chars
- Use different passwords for different domains (Yahoo, Facebook, Snap Chat, UOREGON.EDU)
- Change them regularly – at least every 6 months
- Use a password manager (like KeyPass or LastPass)

- Never use login as password
- Never store them under keyboards, desk drawers, sticky notes on monitor
- Store a clue in your wallet/purse
- Never store them on refrigerator
- Never ever share passwords with anyone!
- Never send them in email
- Never enter them with a “shoulder surfer” present
Dangers of malware…

- to YOU
  - Webcam spyware
  - Key logger
  - Virus
  - Secrets

- to OTHERS
  - Bots
  - Zombies
  - Data breach
How do I get infected?

- social engineering via email, instant messaging, social media
- malicious websites and drive-by downloads, P2P file sharing
- malvertising, man-in-the-middle attacks, exploit kits
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment  Decrypt
General Malware Tips

- Turn on automatic updates on your:
  - Phones
  - Home computers
  - Tablets
  - Work computers (see IT)

- Run up-to-date antimalware tool
  - McAfee
  - MalwareBytes
  - Windows Defender (free)

- Back up important files
- Occasionally try to restore something from backup
- Report suspicious computer activities
- Never download from untrusted websites
- Be careful of sites you browse to!
I STOLE YOUR FACEBOOK LOGIN, CELLPHONE RECORDS & EMAIL PASSWORD

BUT IT'S COOL, YOU HAVE NOTHING TO HIDE, RIGHT?

Protect your SOCIAL BRAND
Social Media tips

- No Internet delete button
- Don't share secrets
- Trust then connect
- Use different passwords for different personas
- Secure device – facial, password, fingerprint, ...
- Setup 2-factor authN
- Turn on privacy settings
- Setup private accounts
- Limit who sees posts
- Limit who can find you
YOU DON'T USE A VPN AT A PUBLIC HOTSPOT?

YOU REALLY DO LIKE TO LIVE DANGEROUSLY!
Insecure connection

intercept...hijack...modify
VPN, https://

secure encrypted tunnel

Evil Wifi

Evil Internet

Photos by Unknown author is licensed under CC BY-SA
International travel tips

**Before you go**
- Backup your system/data
- Remove sensitive data
- Change passwords/PIN
- Update patch and antivirus

**While traveling**
- Physical security
- Shoulder surfers
- No sensitive transactions on public wifi
- No auto-join
- Fake login to test
- Avoid using public devices

**When you return**
- Assume compromise
- Update device
- Update antivirus
- Change all passwords/PINs
Top 5 defenses

- 2FA
- Phishaware
- Passphrase
- Updates
- Backup

Awareness & Vigilance
Key takeaways

1. Don't get mished by a dumb hacker!

2. Make strong passwords or phrases, and never share them with anyone, ever!

3. Always use 2-factor login, where available

Finally, be vigilant but unafraid!
UO Cybersecurity Briefing & Awareness Training

Leo F. Howell
Chief Information Security Officer
lfhowell@uoregon.edu
541-346-1732