

Cybersecurity Awareness Training

be vigilant but unafraid!

Leo F. Howell

Chief Information Security Officer

lhowell@uoregon.edu



UNIVERSITY OF
OREGON

WHY YOU CARE



Why YOU care

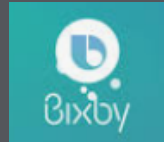
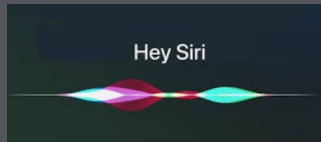
Security & Compliance

1. **COMPLIANCE** increases business: HIPAA, FERPA, GDPR, GLBA, ...
2. **DATA BREACHES** cost money and tarnish reputations
3. **DENIAL OF SERVICE** disrupts operations
4. **YOU**: research, bank account, medical records, embarrassment, etc.



Why YOU care

Your privacy and safety matters!



- “Alexa, delete what I said today”
- Settings > Alexa Account > History
- Turn off microphone and camera
- Keep away from eavesdroppers
- What’s your wake word?
- Google how to secure Alexa, Siri, Bixby, ...

Hack Your car!



Hack Your social life



THREAT UPDATE

A network diagram background consisting of a series of interconnected nodes and lines, forming a complex web structure. The nodes are represented by small black dots, and the lines are thin, light gray lines connecting the nodes. The overall appearance is that of a digital network or data flow.

Common attack methods

- Email – Phishing
- Phone - Vishing
- Text - Smishing

Phishing



- Password theft
- Backdoors
- Website exploits

Hacking



- Ransomware
- Key loggers
- Spyware

Malware



Ooops, your files have been encrypted!

English



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

© 2017 Wana Decrypt0r 2.0



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

[Check Payment](#)
[Decrypt](#)

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Ransomware



Updates
 Backup

Security incidents @ UO

Date	Description	UO Scope
Mar 2019	14 users' direct deposit modified; no paychecks lost	14
Aug 2018	15,000 students, faculty, staff DuckIDs and passwords potentially stolen; cost \$80K (1,300 person-hours)	15,000
Oct 2016	60 Faculty DuckID and passwords stolen by the state-sponsored actors	60
Nov 2017	Phishing Campaign	58
Aug 2017	Phishing Campaign	29
May 2017	WannaCry/Jaff Ransomware	508
April 2016	Website set to incorrect permissions allows anonymous access to data	60

A meme featuring Steve Moss from the TV show 'The Office'. He is in a cubicle, wearing his signature blue shirt, red suspenders, and patterned tie. He is looking at a computer screen (not fully visible) with a slightly skeptical or weary expression. The background shows a typical office environment with cubicles and fluorescent lighting.

YEAH IF WE COULD JUST

**STOP CLICKING ON PHISHING
EMAILS, THAT'D BE GREAT.**

A person wearing a blue long-sleeved shirt and blue shorts is standing on a boat, aiming a compound bow. The bow is green and black. The person is looking towards the water. In the water, several sharks are visible, swimming near the surface. The background shows a vast blue ocean under a clear sky with some light clouds. A dark green horizontal bar is overlaid across the middle of the image, containing the text.

Can you spot the phish?

Spot the Phish!



- Mouse-over before you click
- Fake D0mains ***uoregon.edud***
- Flattery
- Urgency
- Unknown sender
- Unexpected tone
- Unusual request
- Letter Sub5titution5
- Bad Grammra
- 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



"Unable to display message" phishing

From: <[REDACTED]@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](#)

Logo



www-svha.msgload9.icu



UNIVERSITY
OF OREGON

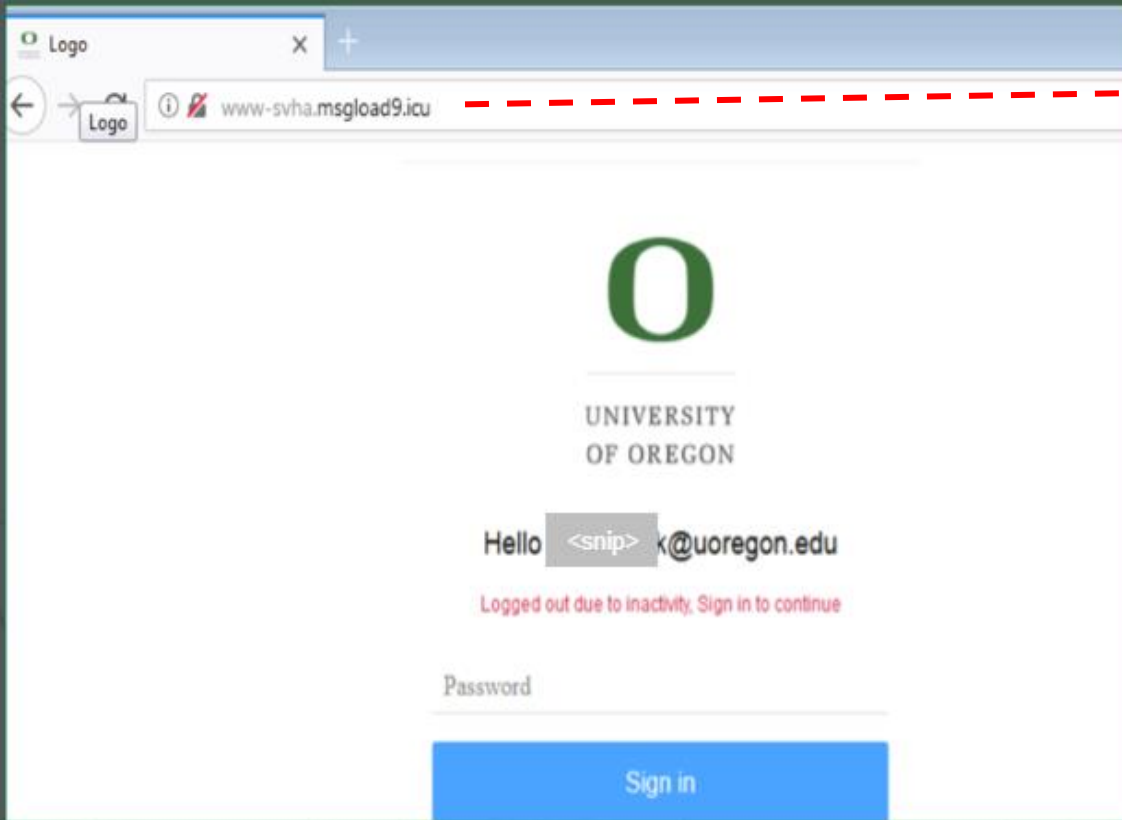
Hello <snip>k@uoregon.edu

Logged out due to inactivity. Sign in to continue

Password

Sign in

"Unable to display message" phishing



www-svha.msgload9.icu

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



Gift card scam with...

From: david.lonover@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.

Dave



Gift card scam with...

From: david.lonover@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.

Dave



Gift card scam...

fake domain, context, urgency.

From: david.lonover@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.

Dave



Take my paycheck!!

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



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

jw13925@my.bristol.ac.uk



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!!



UNIVERSITY OF OREGON
DuckWeb Information System
HELP | EXIT

Welcome to DuckWeb!

⚠ DuckWeb is unavailable Friday evenings from 7pm to 9pm for routine maintenance.

To Login: Enter your UO ID number (do not enter dashes) and your Personal Access Code (PAC), then click on the **Login** button.

First-time Users: Use the UO ID and initial PAC provided to you by the University of Oregon. Once you log in, for security reasons, DuckWeb will display that your PAC has expired and you will be prompted to change your PAC and to activate a security question which will help you manage your account. Click on the **HELP** button above for more information about your PAC.

Forgot your Personal Access Code (PAC)? Don't guess! Enter your UO ID number (no dashes) and click the "Forgot PAC?" button. Follow the steps on the next page. If you forgot the answer to your security question (or if you never created one), further instructions will follow.

UO ID:
PAC:

Login | Forgot PAC?

⚠ **REMEMBER**, especially if you are using a public computer, to Log Off by clicking **EXIT** and then close your browser when you are finished. Avoid using the forward/back buttons on your browser unless specifically directed to do so. For security reasons, DuckWeb requires that your browser be configured to accept **cookies**.

Comments? apolster@uoregon.edu

RELEASE: 8.8.2

© 2019 Ellucian Company L.P. and its affiliates.
This software contains confidential and proprietary information of Ellucian or its subsidiaries.
Use of this software is limited to Ellucian licensees, and is subject to the terms and conditions of one or more written license agreements between Ellucian and such licensees.

http://simoladormil.org/....

https://duckweb.uoregon.edu

https://duckweb.uoregon.edu/pls/prod/twbkwbis.P_WWWLogin

UNIVERSITY OF OREGON
DuckWeb Information System
HELP | EXIT

Welcome to DuckWeb!

⚠ DuckWeb is unavailable Friday evenings from 7pm to 9pm for routine maintenance.

To Login: Enter your UO ID number (do not enter dashes) and your Personal Access Code (PAC), then click on the **Login** button.

First-time Users: Use the UO ID and initial PAC provided to you by the University of Oregon. Once you log in, for security reasons, DuckWeb will display that your PAC has expired and you will be prompted to change your PAC and to activate a security question which will help you manage your account. Click on the **HELP** button above for more information about your PAC.

Forgot your Personal Access Code (PAC)? Don't guess! Enter your UO ID number (no dashes) and click the "Forgot PAC?" button. Follow the steps on the next page. If you forgot the answer to your security question (or if you never created one), further instructions will follow.

UO ID:
PAC:

Login | Forgot PAC?

⚠ **REMEMBER**, especially if you are using a public computer, to Log Off by clicking **EXIT** and then close your browser when you are finished. Avoid using the forward/back buttons on your browser unless specifically directed to do so. For security reasons, DuckWeb requires that your browser be configured to accept **cookies**.

Comments? apolster@uoregon.edu

RELEASE: 8.8.2

© 2019 Ellucian Company L.P. and its affiliates.
This software contains confidential and proprietary information of Ellucian or its subsidiaries.
Use of this software is limited to Ellucian licensees, and is subject to the terms and conditions of one or more written license agreements between Ellucian and such licensees.

Dangerous | https://simoladormil.org/wp-content/stoic/outlookwebapp.html

allow scripts to run. For information about how to allow scripts, consult the Help for your browser. If your browser does not allow scripts to run, you will not be able to use Outlook Web App.

Outlook® Web App

User name:

Password:

sign in

1

2

3



From: University of Oregon <jw13925@my.bristol.ac.uk>

Sent: Wednesday, March 6, 2019 9:57 AM

To: George Reese

Subject: Important Campus Security Notification



Dear Greese

You are receiving this Important

You have an important notification
information below immediately for

[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

DEFENSE

The image features a dark gray background. A prominent horizontal green band runs across the middle. The word "DEFENSE" is written in large, white, sans-serif capital letters, centered within this green band. Below the green band, a network diagram is visible, consisting of numerous small black dots (nodes) connected by thin, light gray lines, creating a complex web of connections.

Device Loaner Program

- Travel to high-risk countries

Afghanistan, Armenia, Azerbaijan, Belarus, China, Cuba, Georgia, Hong Kong, India, Iraq, Israel, Kazakhstan, Kyrgyzstan, Lebanon, Libya, Macau, Mali, Moldova, North Korea, Pakistan, Russia, Saudi Arabia, Somalia, South Sudan, Taiwan, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Venezuela, Yemen

- MacBooks and Windows Laptops
- How does it work? We identify the traveler in Concur and notify them and their travel delegates of the program.



Welcome to the UO Phish Tank

UO Phish Tank

Exposing phishing scams for the UO community.



- Quickly find foiled phishing messages
- Also see legitimate messages that look like phishing

<https://phishtank.uoregon.edu>



URL Link Protection

Nominations for officer of administration awards due Aug. 19

The awards recognize OAs who make positive impacts to the university

[https://urldefense.com/v3/https://t.e2ma.net/click/gmzedc/w6p93g/4gfqwq_!5W9E9PnL_ac!UFI70Ky_A4Q7qEbHISIAU8FkTHdLij14GHWPSwBCezr-oJOGb6TSIW2CbSTyiheQ\\$](https://urldefense.com/v3/https://t.e2ma.net/click/gmzedc/w6p93g/4gfqwq_!5W9E9PnL_ac!UFI70Ky_A4Q7qEbHISIAU8FkTHdLij14GHWPSwBCezr-oJOGb6TSIW2CbSTyiheQ$)

Bloomberg Law, Elizabeth Tippet, associate professor, School of Law

Juneau Empire, Madonna



Web Site Has Been Blocked!

The web page you are attempting to access has been classified as malicious. This classification is determined by direct analysis of the web page. Although an entire web site may be blocked as malicious, it is very common for a single page on a valid web site to be blocked.

Your organization has enabled this technology to protect you, your system, and the organization from harm. Blocked pages contain material such as:

- **Credential Theft:** A page may be designed to look like a valid financial institution, a well-known organization, or an otherwise trusted source. The page is requesting a login and/or password for malicious purposes.
- **Malware:** A page may contain files or other malicious material which are intended to harm your system or organization. The malicious material may contain a virus, an installation program, or it may expose a vulnerability in a program which exists on your system.

All external links are evaluated and blocked if high likelihood of maliciousness.



PASSWORDS

The image features a dark gray background. A prominent horizontal green band runs across the middle. The word "PASSWORDS" is written in large, white, sans-serif capital letters across this band. Below the band, a network diagram is visible, consisting of numerous small black dots (nodes) connected by thin, light gray lines, creating a complex web of connections.

P@55W0rd5!

Good Ones

W@r 15 b@d @1w@y5	Strong (76)
My 3y3s @r3 pink	Strong (70)
This is my story	Strong (69)
What is fake news?	Strong (87)
My secret bucket list item is to sing in public	Very Strong (217)
I hate math, but I totally dig chemistry	Very Strong (197)

Bad Ones

123456
Letmein
Football
Iloveyou
Admin
Welcome
Monkey
Abc123
hello
Starwars

- Time, 2017

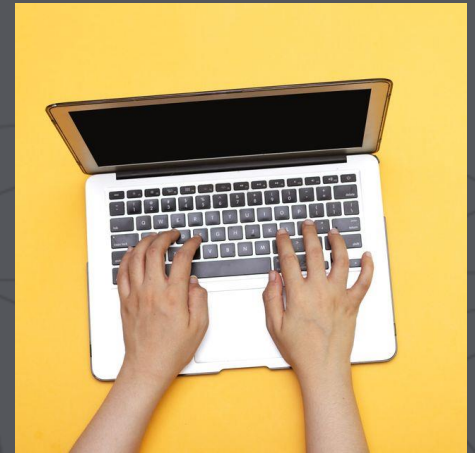


General password tips

- 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



MOBILE DEVICES



Basic Mobile Device Security

- Screen lock (PIN)
- SIM card lock (PIN)
- Turn off Bluetooth when not in use; decline pairing requests
- Turn off geotagging
- Hard drive encryption
- Strong cloud password
- Backup to cloud
- Enable remote wipe



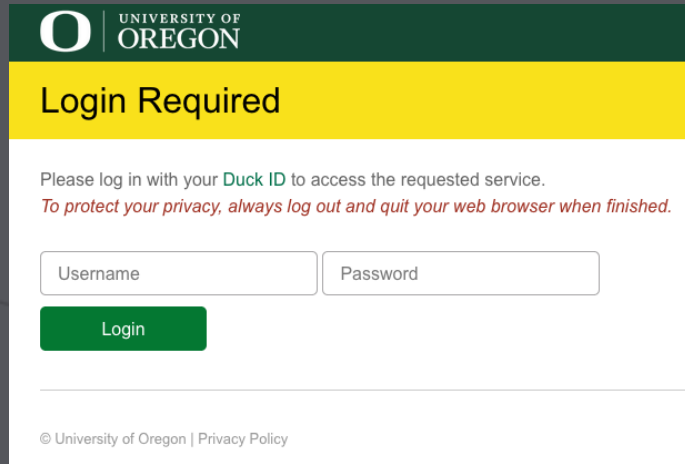
Two-Step Login

Something you know (password, PIN, security questions)

Something you have (phone, token)

Something you are (fingerprint, iris, palm, face)

Something you have



UNIVERSITY OF OREGON

Login Required

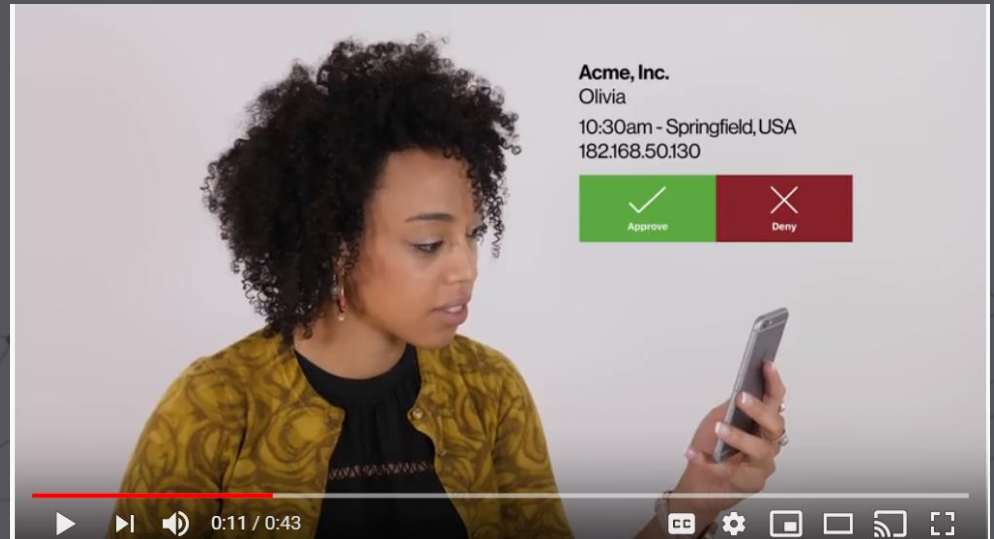
Please log in with your **Duck ID** to access the requested service.
To protect your privacy, always log out and quit your web browser when finished.

Username Password

Login

© University of Oregon | Privacy Policy

Something you know



FAQ on mobile & email

1. Should I forward my email to an outside email like Yahoo, Google, Att, etc.? **No**
2. Can Information Services **wipe** my phone if I install the Outlook client? **We won't**
3. Will my phone be **discoverable** if I use it for two-step login? **No**



IT'S A WRAP



Top 5 defenses



2FA



Phishaware



Passphrase



Updates



Backup

Awareness & Vigilance

UO Cybersecurity Awareness Training

Leo F. Howell

Chief Information Security Officer

lhowell@uoregon.edu

541-346-1732



UNIVERSITY OF
OREGON