

Cybersecurity Awareness Training

be vigilant but unafraid!

Leo F. Howell

Chief Information Security Officer

lhowell@uoregon.edu



UNIVERSITY OF
OREGON

Why YOU should care

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



Hacktivism?



Hacktivist?



Insiders



Organized Crimes



Nation States

Common attack methods

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

Phishing



- Password theft
- Backdoors
- Website exploits

Hacking



- Ransomware
- Key loggers
- Spyware

Malware



YEAH IF WE COULD JUST

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

Can you spot the phish?



1. Fake D0mains *uoregon.edud*
2. Urgency
3. Impersonated / Unknown Sender
4. Unexpected Tone / Request
5. Flattery
6. Letter Sub5titution5
7. Bad Grammra



Phishing-4-faculty with...

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:*

<http://shibboleth.uoregon.edud.in/idp/Authn/login.php?url=http://www.sciencedirect.com/science/article/pii/S03085961100HT00238>

*Thanks for you Cooperation in Advance.
Assoc. Prof. [Name]*

Phishing-4-faculty with...

flattery, grammar, fake domain, urgency

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:

<http://shibboleth.uoregon.edud.in/idp/Authn/login.php?url=http://www.sciencedirect.com/science/article/pii/S03085961100HT00238>

Thanks **for you C**ooperation in **A**dvance.
Assoc. Prof. [Name]

Phishing-4-facult flattery, grammar, fak

Dear Dr. [X],

I recently read your article: [Tit
research. I wonder, if pos
current research:

<http://shibboleth.uoregon.edu/ect.com/science/article/pii/S03>

Thanks for you Cooperation in
Assoc. Prof. [Name]

- **\$3.4B** IP Theft
- **3,800** Professors targeted, across
- **144** U.S. universities
- **10** Indictments
- **n UO Faculty & Staff Compromised**

Phishing-4-whales with...

From: Michael Schill [mailto:markross@[emailolympic.org](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

Open = <http://ko-ontap.com/cat/index.html>

Kindly let me have your opinion

Michael Schill

541-346-3936

President

Gift card scam with...

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



Gift card scam...

fake domain, context, urgency.

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@uoregon.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



Safari malware...

From: andrea@uoregon.edu

Hello You,



http://click_to_download_malware.badPlace.com

Must see pictures from my safari tour.

<http://dropbox.com/andrea@safari>. Don't share, I am embarrassed about a few of them.

Andrea



Bad CISO...

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



Bad CISO

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.edu/d.in>.

Thank you,

CISO's Office



Dumb hacker!

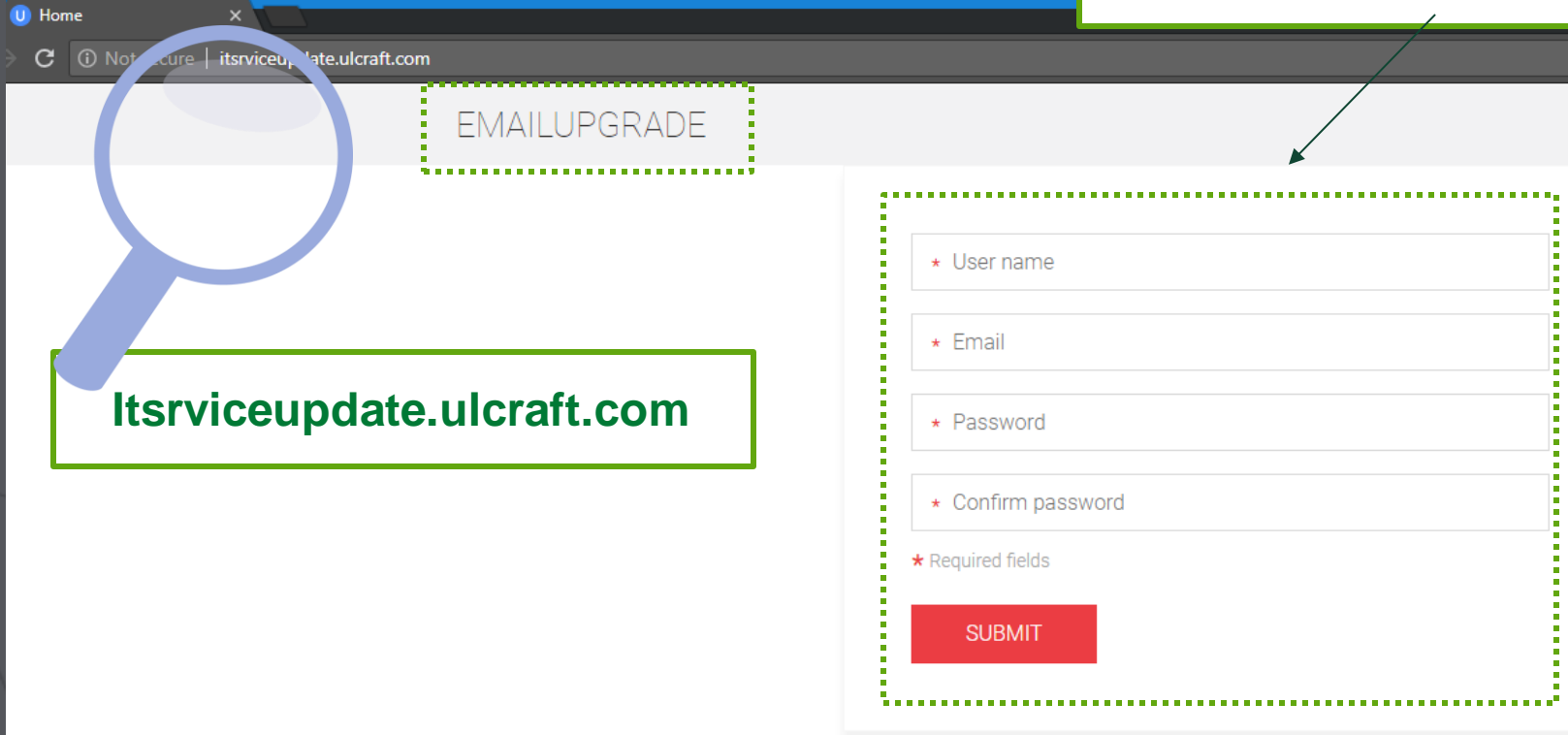
From: Mirian Livia Oliveria <mirian.oliveria@cultra.gov.br>

Your Password have expired [CLICK HERE](#) to verify



Dumb phish!

What's missing?



The image shows a browser window displaying a phishing page. The address bar shows the URL `itserviceupdate.ulcraft.com`. The page header contains the text "EMAILUPGRADE". A magnifying glass highlights the URL in the address bar, which is also enclosed in a green box with the text "Itserviceupdate.ulcraft.com". A green dashed box highlights the registration form, which includes fields for "User name", "Email", "Password", and "Confirm password", a "Required fields" note, and a red "SUBMIT" button. A green box at the top right contains the text "What's missing?" with an arrow pointing to the registration form area.

Home

Not secure | itserviceupdate.ulcraft.com

EMAILUPGRADE

* User name

* Email

* Password

* Confirm password

* Required fields

SUBMIT

Itserviceupdate.ulcraft.com



"Unable to display message" phish

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

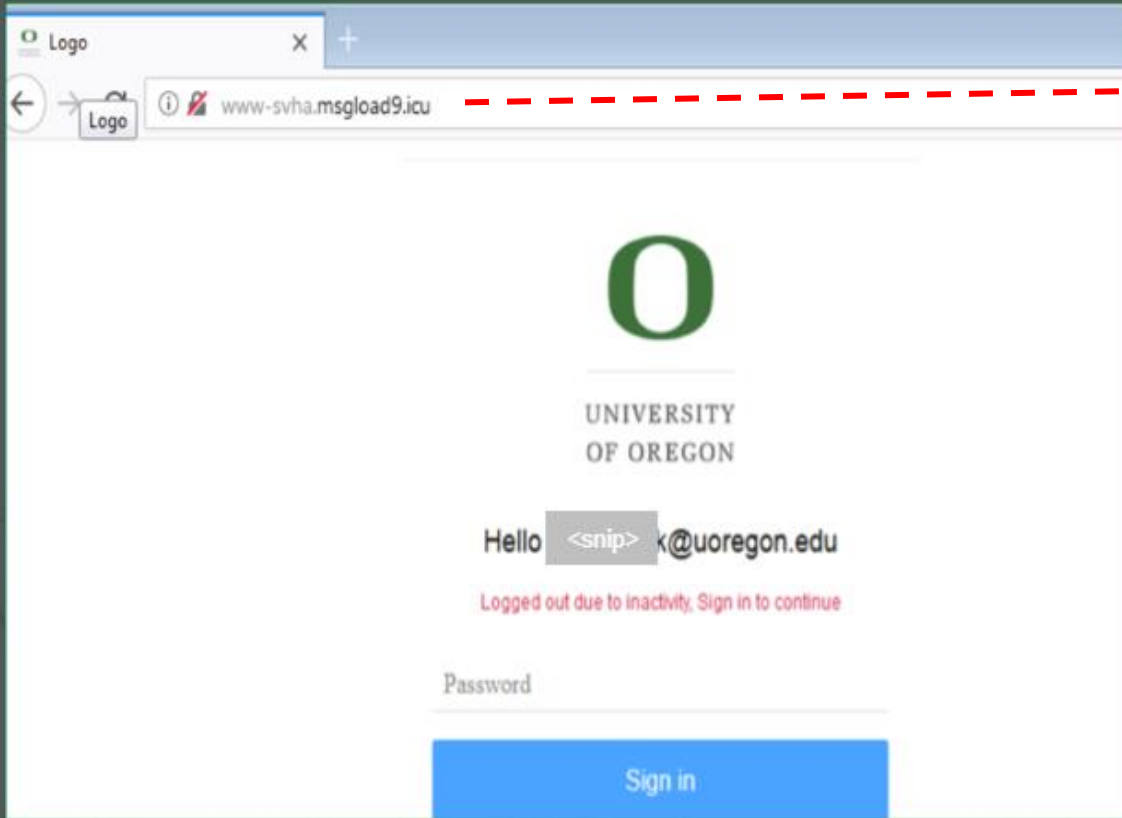
Hello <snip>k@uoregon.edu

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



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 may not be able to use the 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

General phishing tips



- 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***



Key Message on Phishing

Don't get Phished, Smished, Vished

By a....

Dumb Hacker!



Password too long to
remember?

GOOD.

Use...
**STRONG
PASSWORDS**



Password game

Good Ones

W@r 15 b@d @1w@y5	Strong (76)
My 3y3s @r3 p1nk	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



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:

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:

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:

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:

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:

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



GOOD GOOD



**ACCEPT THE FREE UPGRADE TO
WINDOWS 10**

imgenerator.net

**Trojans
Viruses
Bots
Zombies
Ransomware**



Dangers of malware...

to
YOU

to
OTHERS

Webcam
spyware

Key logger

virus

Secrets

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!

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

GMT from Monday to Friday

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](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Ransomware



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?!**

WeKnowMemes

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



A meme featuring Gene Wilder as Willy Wonka. He is wearing his signature red suit and black-rimmed glasses, looking slightly to the side with a smug, knowing expression. The background is dark and out of focus, suggesting an indoor setting.

**YOU DON'T USE A VPN
AT A PUBLIC HOTSPOT?**

**YOU REALLY DO LIKE
TO LIVE DANGEROUSLY!**

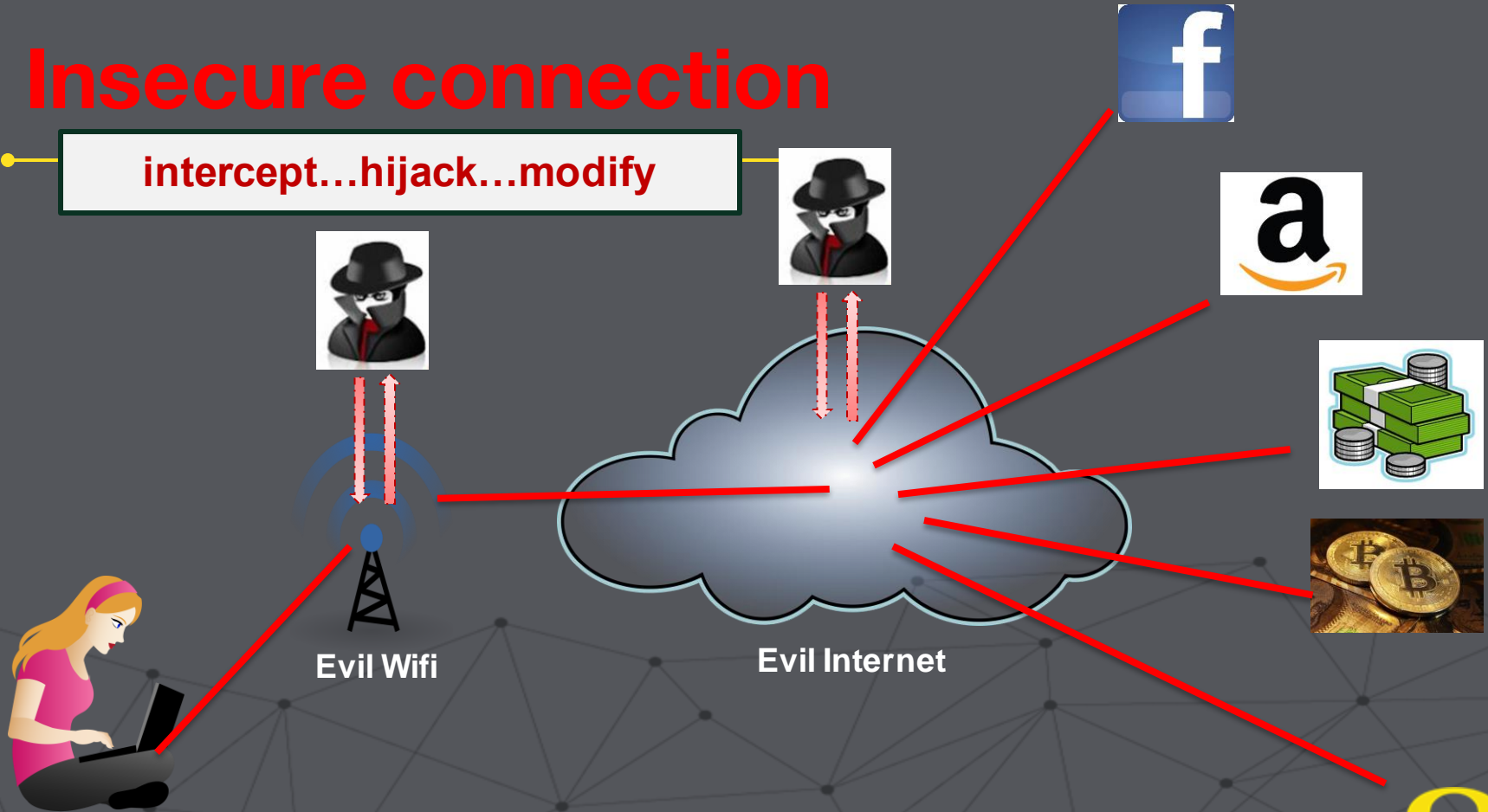
imgflip.com

Protect your
COMMUNICATION



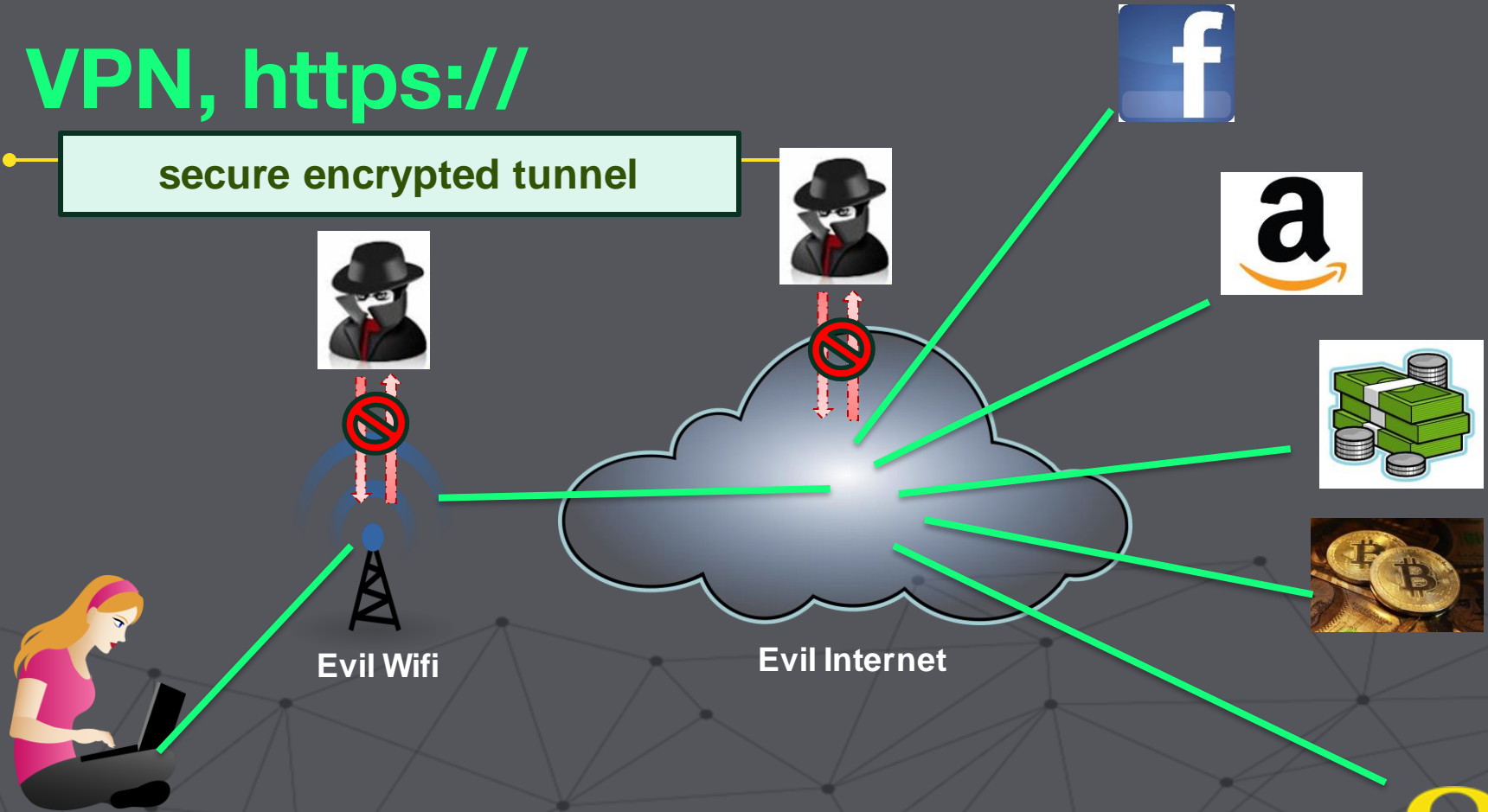
Insecure connection

intercept...hijack...modify



VPN, https://

secure encrypted tunnel



International travel tips

Before you go

- ✓ Backup your system/data
- ✓ Remove sensitive data
- ✓ Change passwords/PIN
- ✓ Update patch and antivirus

When you return

- ✓ Assume compromise
- ✓ Update device
- ✓ Update antivirus
- ✓ Change all passwords/PINs

While traveling

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



Top 5 defenses



2FA



Phishaware



Passphrase



Updates



Backup

Awareness & Vigilance

Key takeaways

1. Don't get ?hished 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



UNIVERSITY OF
OREGON