Internet Safety & Security

University of Alaska Statewide Professional Development Day
August 18, 2017

What are we going to talk about?

Safety and Security on the Internet

Who is out to get me?

How do they do this stuff?

Where are some places I might need to be careful?

What about while I am at work?

What is OIT Security doing to protect us?

What can I do to help keep the University and students safe?

Questions

Who is out to get me?

It is not paranoia if they are really out to get you. - Enemy of the State tagline

- Organized crime
- State sponsored actors
- Hacktivists
- Not so organized crime

WHAT IF I TOLD YOU
YOU'VE BEEN BREACHED?
(AND DIDN'T EVEN KNOW IT)
imgflip.com

How do they do this stuff?

Social engineering

Malware

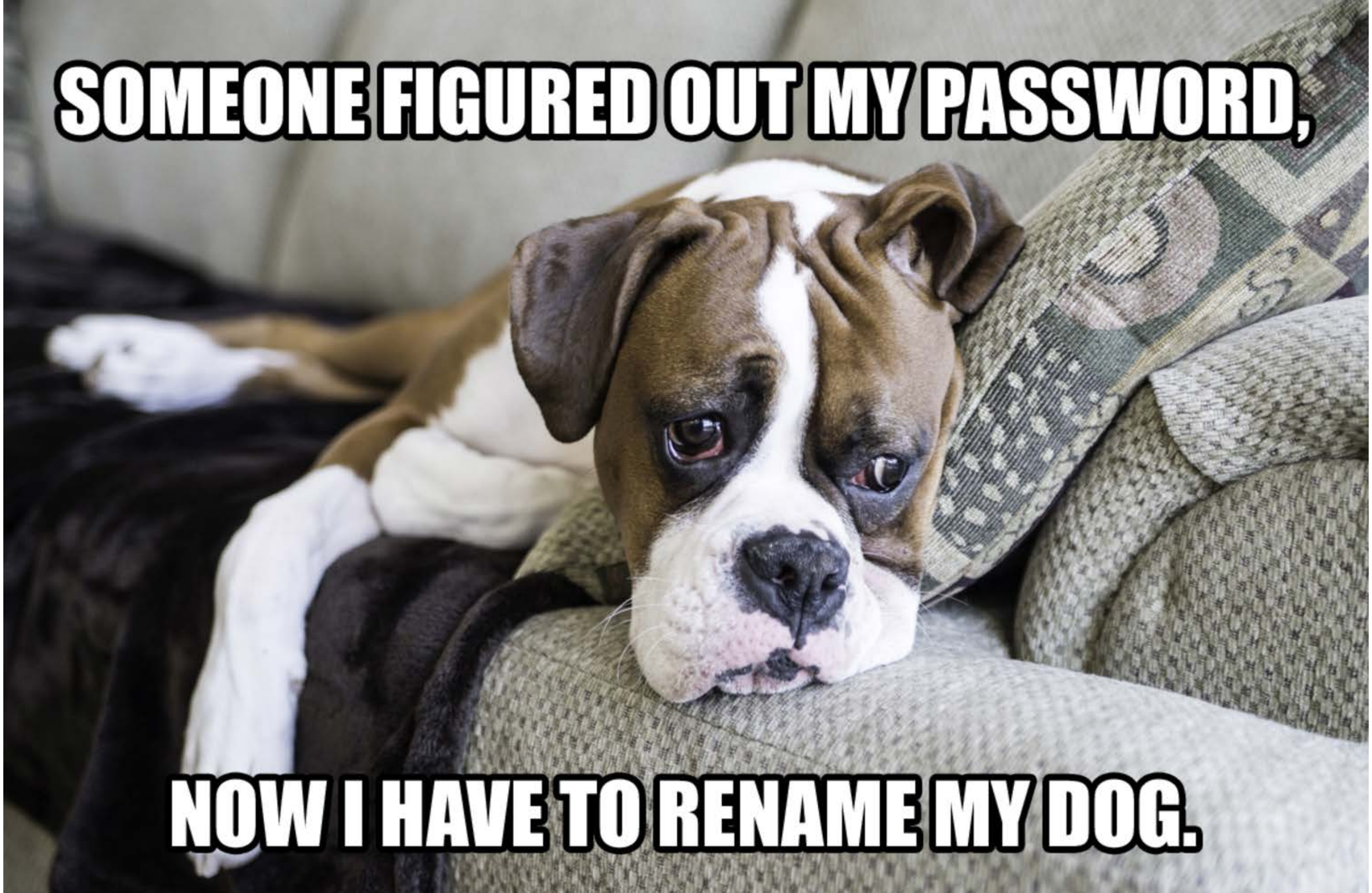
Man-in-the-Middle Attacks

Advanced Persistent Threats

Physical theft

Dumpster diving

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
WAIT FOR IT
Enter your bank account number.
SCAM.
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Dilbert.com DilbertCartoonist@gmail.com
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick


SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

That sounds scary. Where do I need to watch out for this stuff?

Your email inbox!

On the web

On strange networks

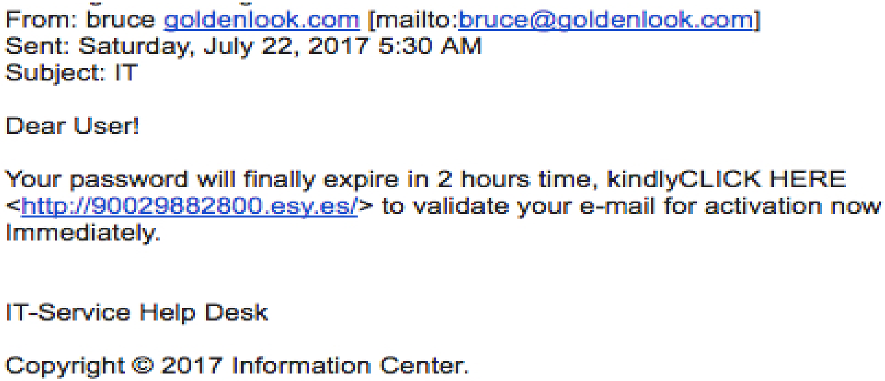
Walking down the street

On social media

Phishing, vishing, & whaling

SPAM was annoying, these are designed to rob you or loot an organization.

- **Phishing - soliciting sensitive information using deception via email**
- **Vishing - soliciting sensitive information using deception via voice communications**
- **Whaling - CEO or other fraud designed to steal or divert large sums of money**



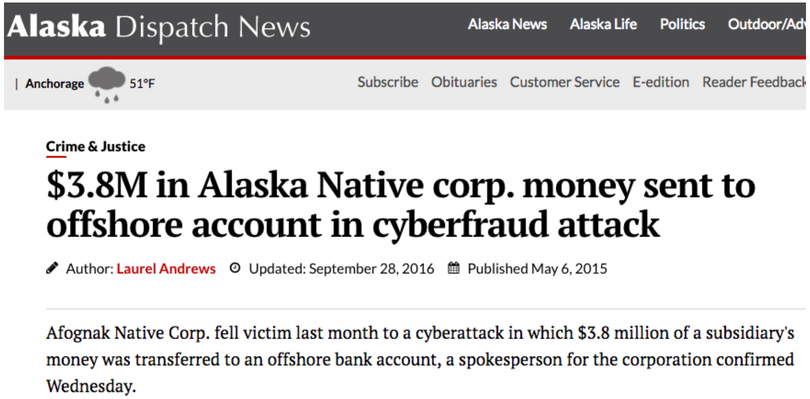
From: bruce goldenlook.com [mailto:bruce@goldenlook.com]
Sent: Saturday, July 22, 2017 5:30 AM
Subject: IT

Dear User!

Your password will finally expire in 2 hours time, kindlyCLICK HERE <http://90029882800.esy.es/> to validate your e-mail for activation now Immediately.

IT-Service Help Desk

Copyright © 2017 Information Center.



Crime & Justice

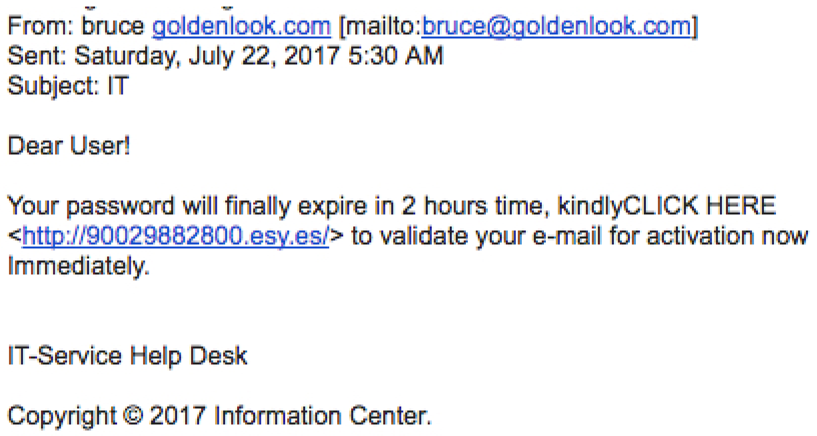
$3.8M in Alaska Native corp. money sent to offshore account in cyberfraud attack

Author: Laurel Andrews Updated: September 28, 2016 Published May 6, 2015

Afognak Native Corp. fell victim last month to a cyberattack in which $3.8 million of a subsidiary's money was transferred to an offshore bank account, a spokesperson for the corporation confirmed Wednesday.

Anatomy of Phishing

1. Generic greeting “Dear User!”
2. The “From:” line and signature do not quite match.
3. The message uses fear, coercion or incentive to get the reader to take an action.
4. URLs are obscured
5. The site you end up at is not the organization's domain name (alaska.edu vs. alaxka.ebu)
6. Use of jargon or department names not a part of the organization



From: bruce goldenlook.com [mailto:bruce@goldenlook.com]
Sent: Saturday, July 22, 2017 5:30 AM
Subject: IT

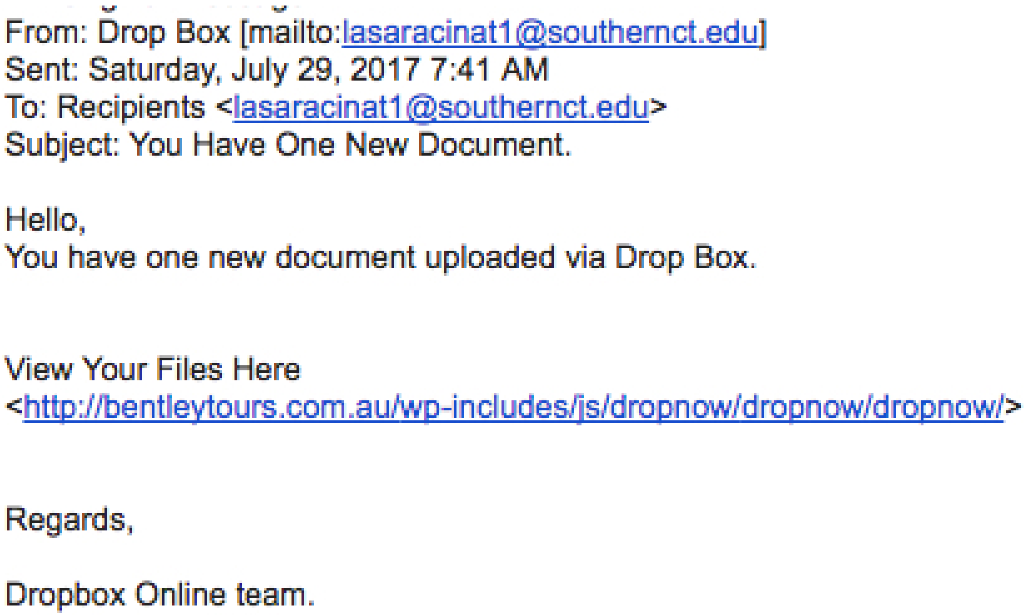
Dear User!

Your password will finally expire in 2 hours time, kindlyCLICK HERE <http://90029882800.esy.es/> to validate your e-mail for activation now Immediately.

IT-Service Help Desk

Copyright © 2017 Information Center.

Real or Phishing?



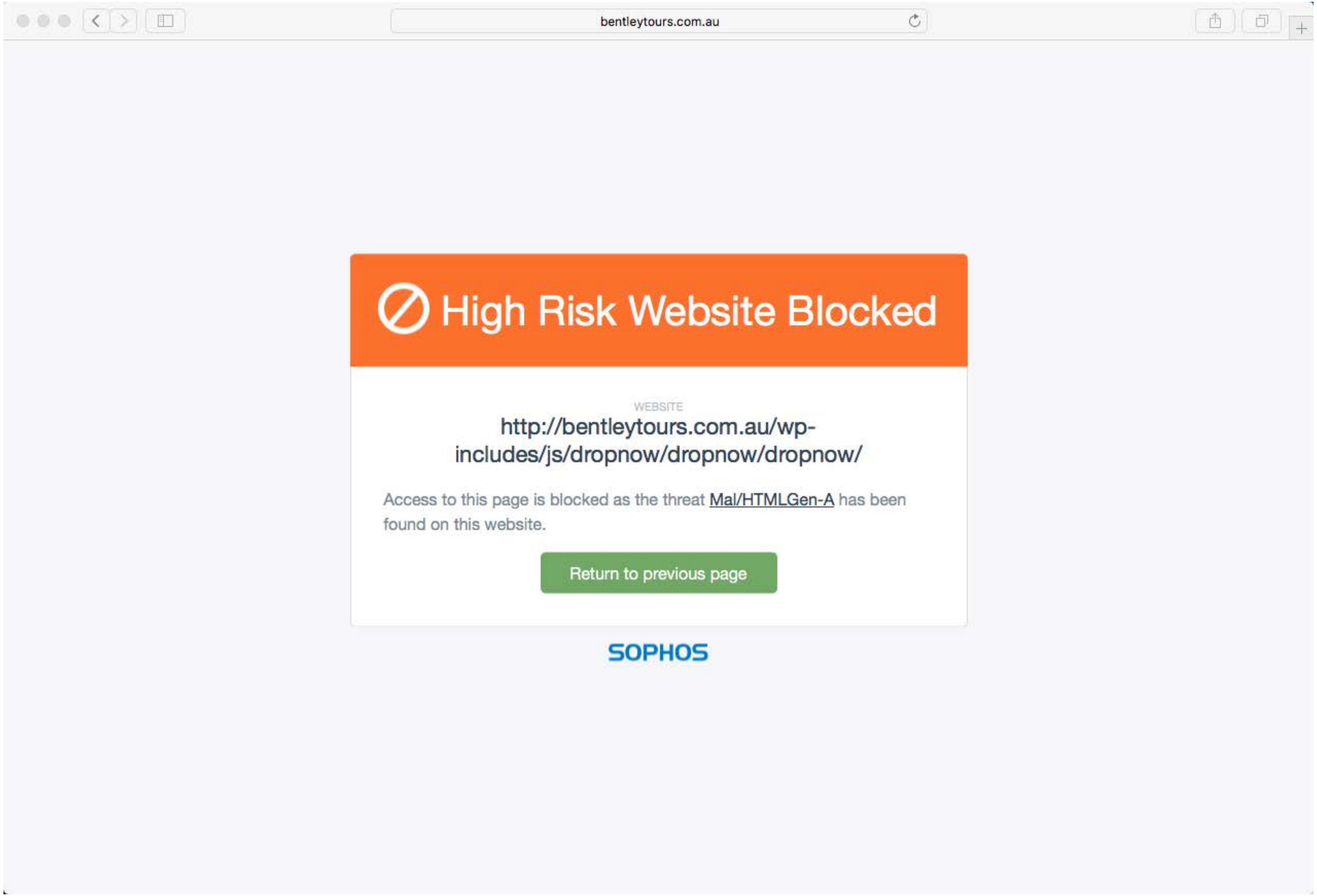
From: Drop Box [mailto:lasaracinat1@southernct.edu]
Sent: Saturday, July 29, 2017 7:41 AM
To: Recipients <lasaracinat1@southernct.edu>
Subject: You Have One New Document.

Hello,
You have one new document uploaded via Drop Box.

View Your Files Here
<http://bentleytours.com.au/wp-includes/js/dropnow/dropnow/dropnow/>

Regards,

Dropbox Online team.



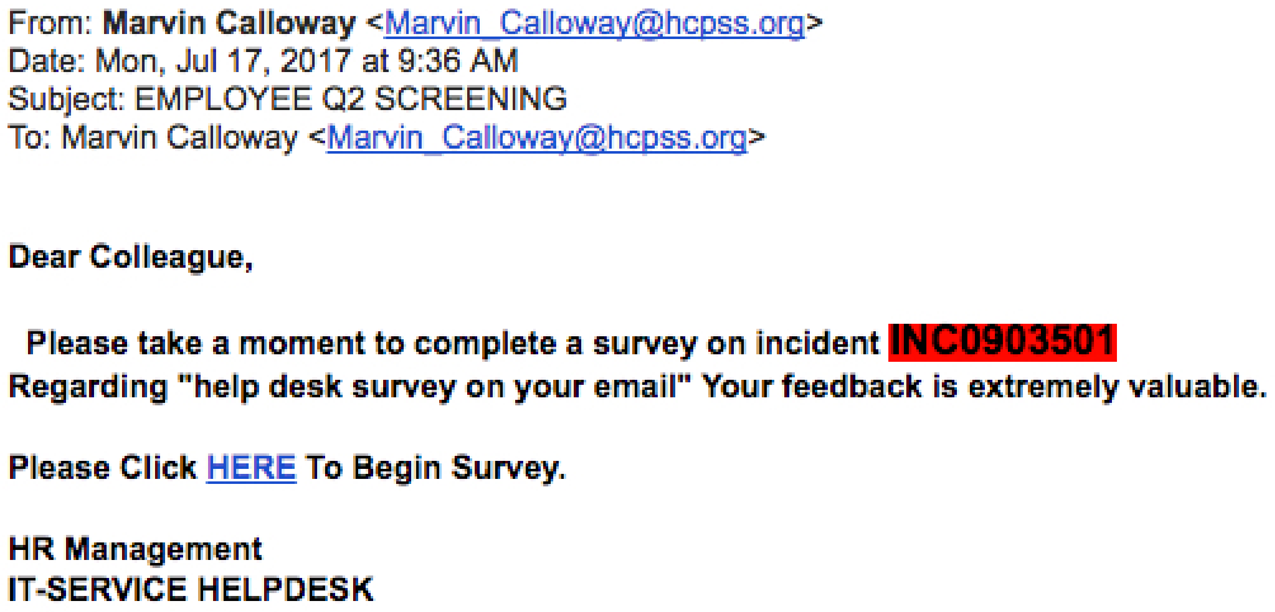
⊘ High Risk Website Blocked

WEBSITE

http://bentleytours.com.au/wp-includes/js/dropnow/dropnow/dropnow/

Access to this page is blocked as the threat Mal/HTMLGen-A has been found on this website.

Real or Phishing?



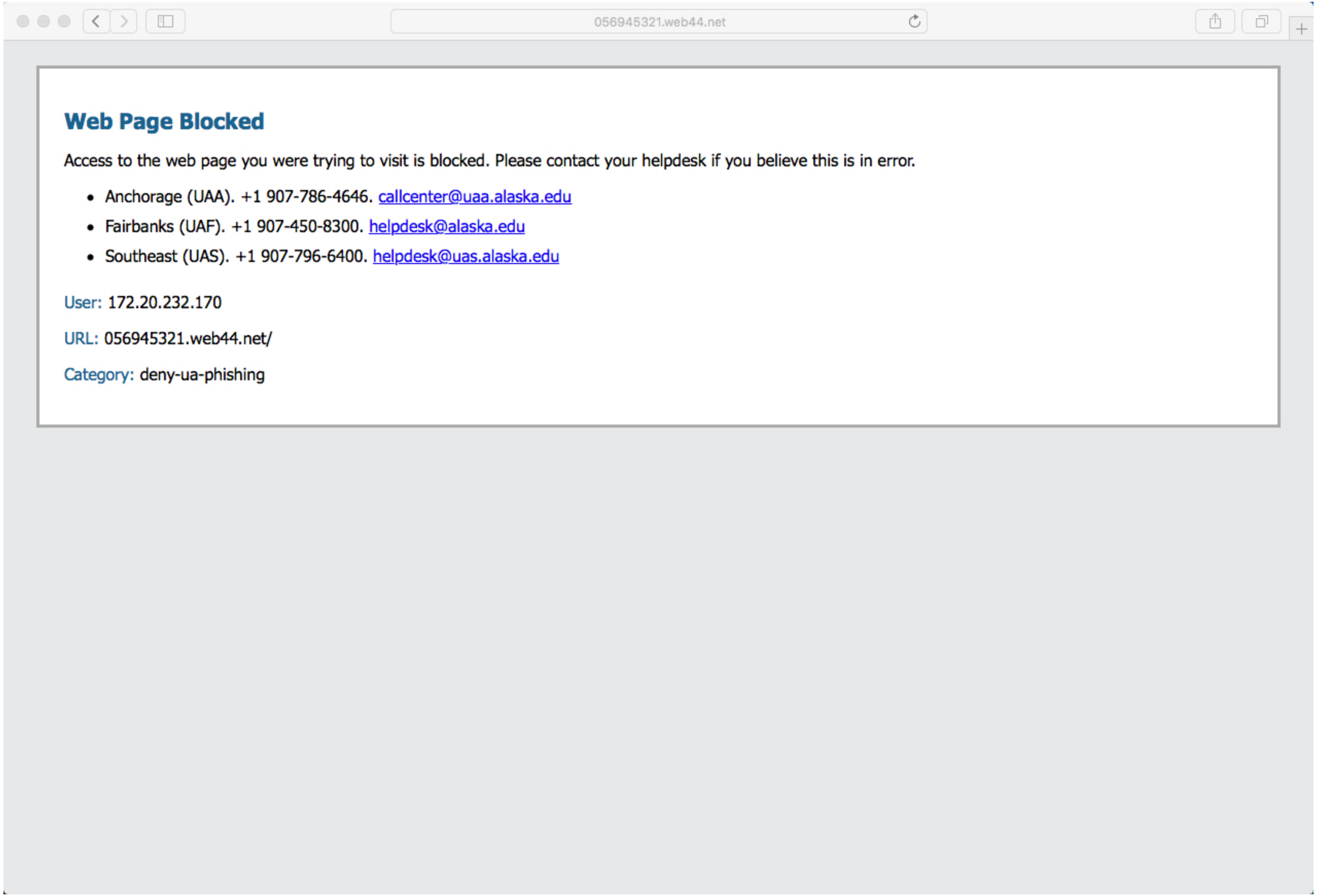
From: **Marvin Calloway** <Marvin_Calloway@hcpss.org>
Date: Mon, Jul 17, 2017 at 9:36 AM
Subject: EMPLOYEE Q2 SCREENING
To: Marvin Calloway <Marvin_Calloway@hcpss.org>

Dear Colleague,

Please take a moment to complete a survey on incident INC0903501 Regarding "help desk survey on your email" Your feedback is extremely valuable.

Please Click HERE To Begin Survey.

HR Management
IT-SERVICE HELPDESK



Web Page Blocked

Access to the web page you were trying to visit is blocked. Please contact your helpdesk if you believe this is in error.

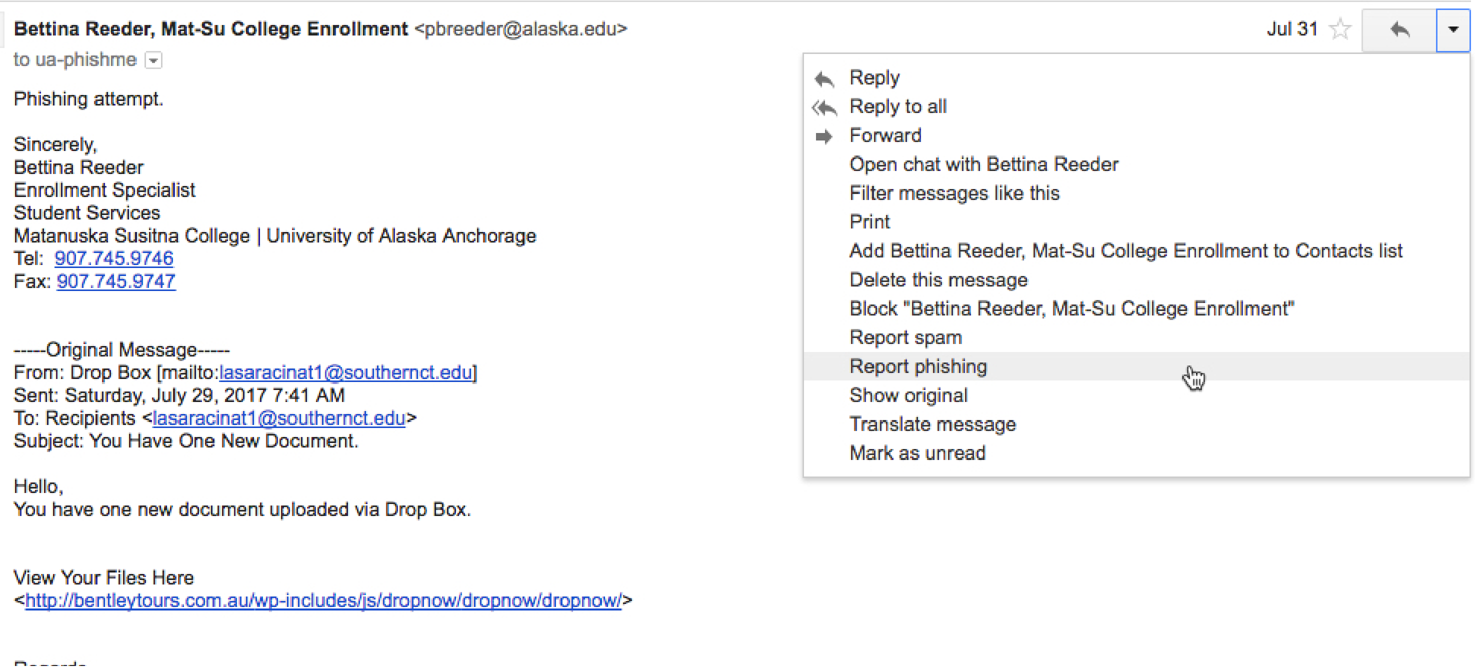
- Anchorage (UAA). +1 907-786-4646. callcenter@uaa.alaska.edu
- Fairbanks (UAF). +1 907-450-8300. helpdesk@alaska.edu
- Southeast (UAS). +1 907-796-6400. helpdesk@uas.alaska.edu

User: 172.20.232.170

URL: 056945321.web44.net/

Category: deny-ua-phishing

Flag as Phishing in Google Mail



Bettina Reeder, Mat-Su College Enrollment <pbreeder@alaska.edu>
to ua-phishme

Phishing attempt.

Sincerely,
Bettina Reeder
Enrollment Specialist
Student Services
Matanuska Susitna College | University of Alaska Anchorage
Tel: 907.745.9746
Fax: 907.745.9747

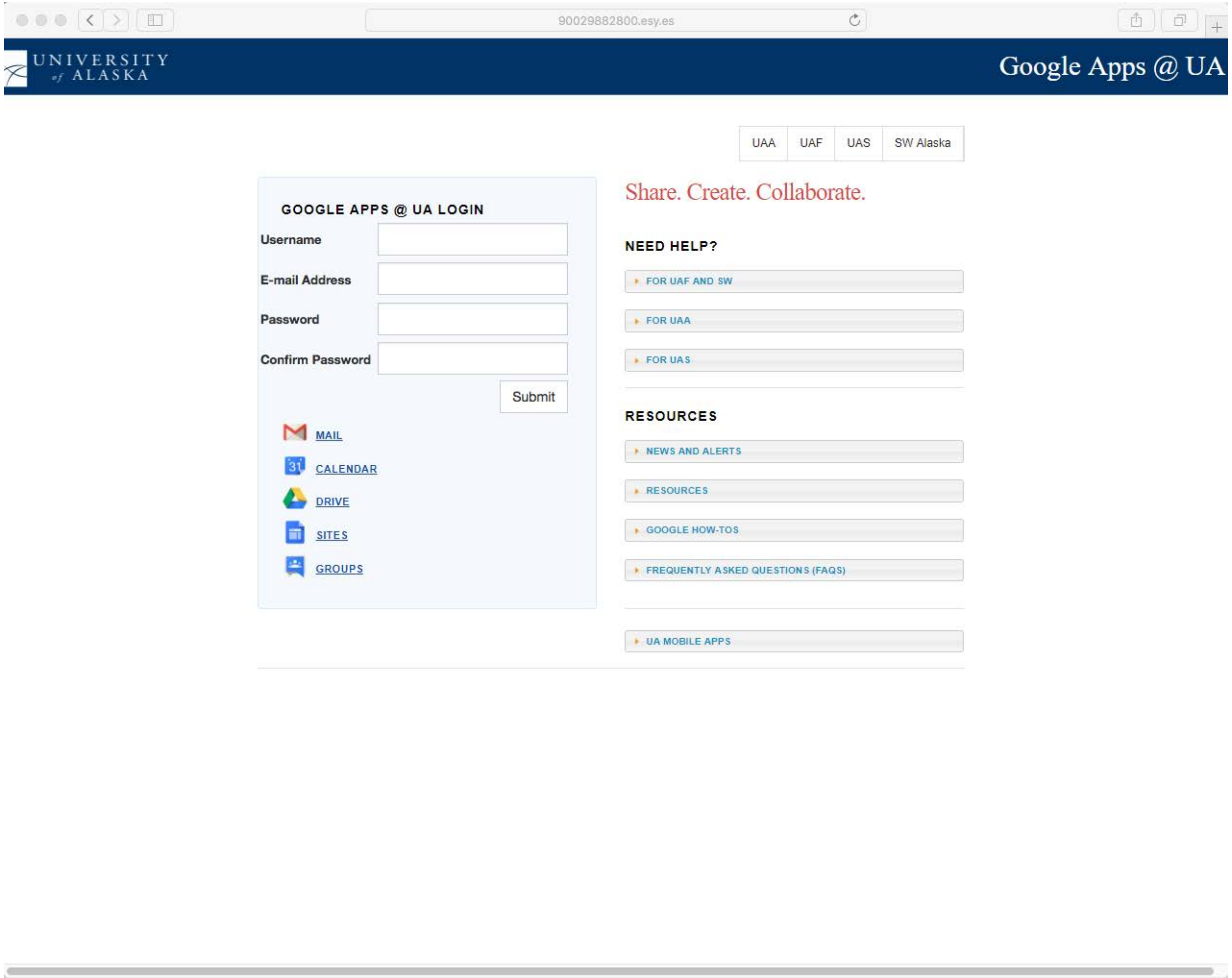
-----Original Message-----
From: Drop Box [mailto:lasaracinat1@southernct.edu]
Sent: Saturday, July 29, 2017 7:41 AM
To: Recipients <lasaracinat1@southernct.edu>
Subject: You Have One New Document.

Hello,
You have one new document uploaded via Drop Box.

View Your Files Here
<http://bentleytours.com.au/wp-includes/js/dropnow/dropnow/dropnow/>

Jul 31
Reply
Reply to all
Forward
Open chat with Bettina Reeder
Filter messages like this
Print
Add Bettina Reeder, Mat-Su College Enrollment to Contacts list
Delete this message
Block "Bettina Reeder, Mat-Su College Enrollment"
Report spam
Report phishing
Show original
Translate message
Mark as unread

Ours or Theirs?



90029882800.esy.es

UNIVERSITY of ALASKA

Google Apps @ UA

GOOGLE APPS @ UA LOGIN

Username

E-mail Address

Password

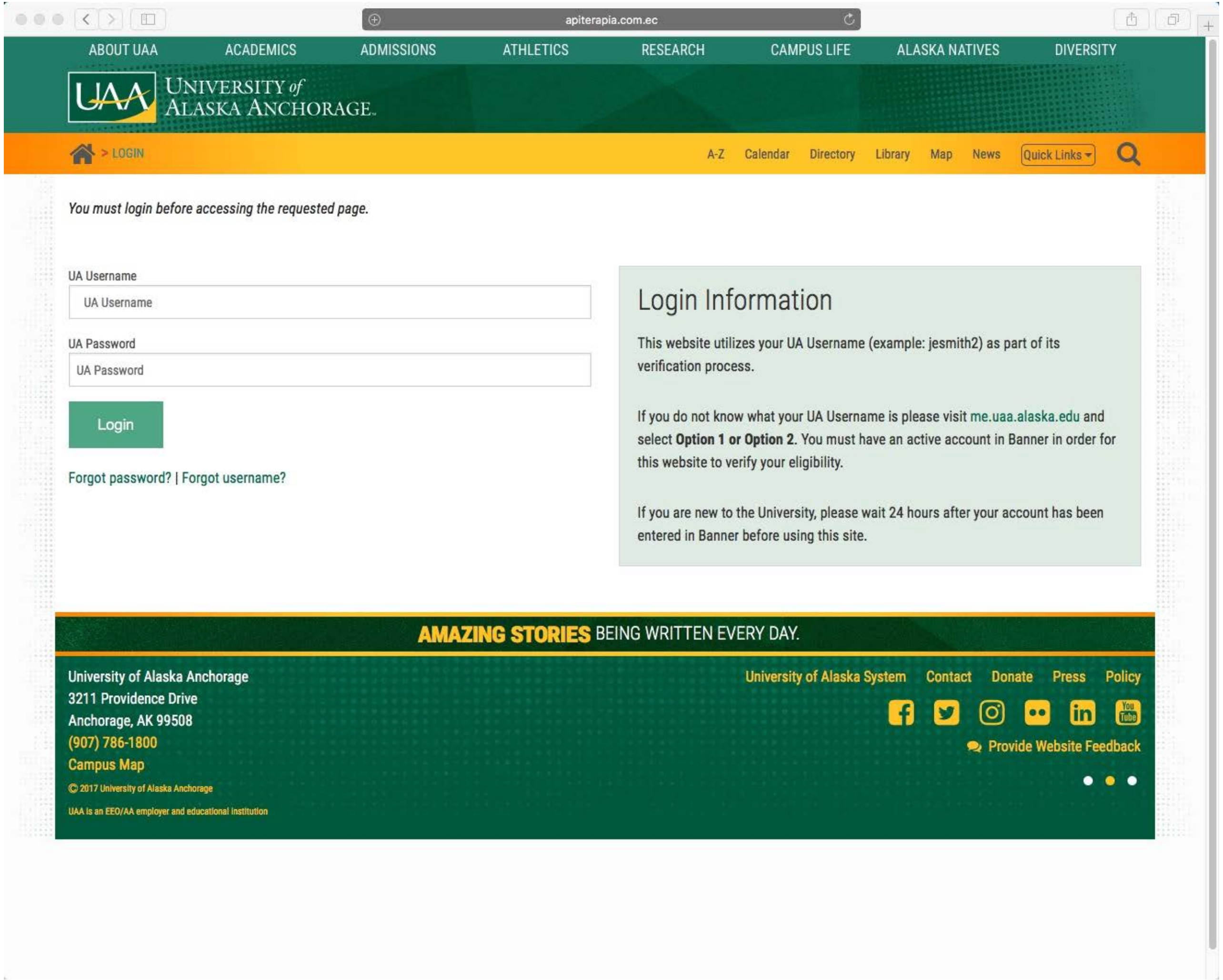
Confirm Password

Share. Create. Collaborate.

NEED HELP?

RESOURCES

Ours or Theirs?



You must login before accessing the requested page.

UA Username

UA Username

UA Password

UA Password

Login

Forgot password? | Forgot username?

Login Information

This website utilizes your UA Username (example: jesmith2) as part of its verification process.

If you do not know what your UA Username is please visit me.uaa.alaska.edu and select **Option 1 or Option 2**. You must have an active account in Banner in order for this website to verify your eligibility.

If you are new to the University, please wait 24 hours after your account has been entered in Banner before using this site.

AMAZING STORIES BEING WRITTEN EVERY DAY.

University of Alaska Anchorage
3211 Providence Drive
Anchorage, AK 99508
(907) 786-1800
Campus Map

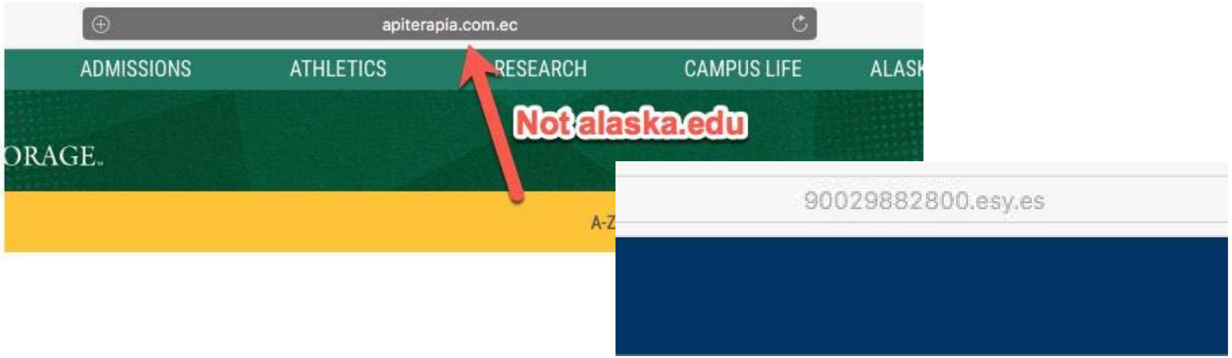
© 2017 University of Alaska Anchorage

UAA is an EEO/AA employer and educational institution

University of Alaska System | Contact | Donate | Press | Policy

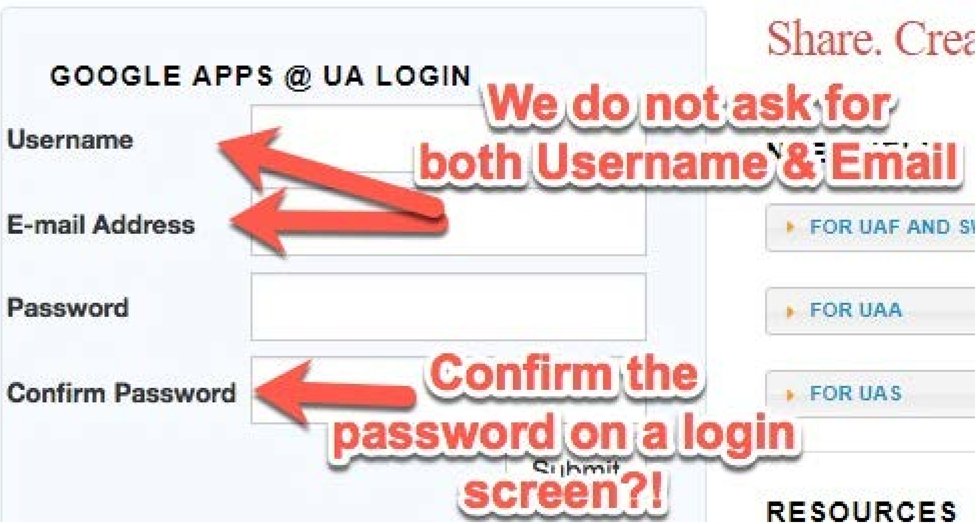
Provide Website Feedback

How can we tell?



Not alaska.edu

1. Check the URL
2. Look for a secure connection (https:// or the lock icon)
3. Does the page look different?
4. How did you get here?

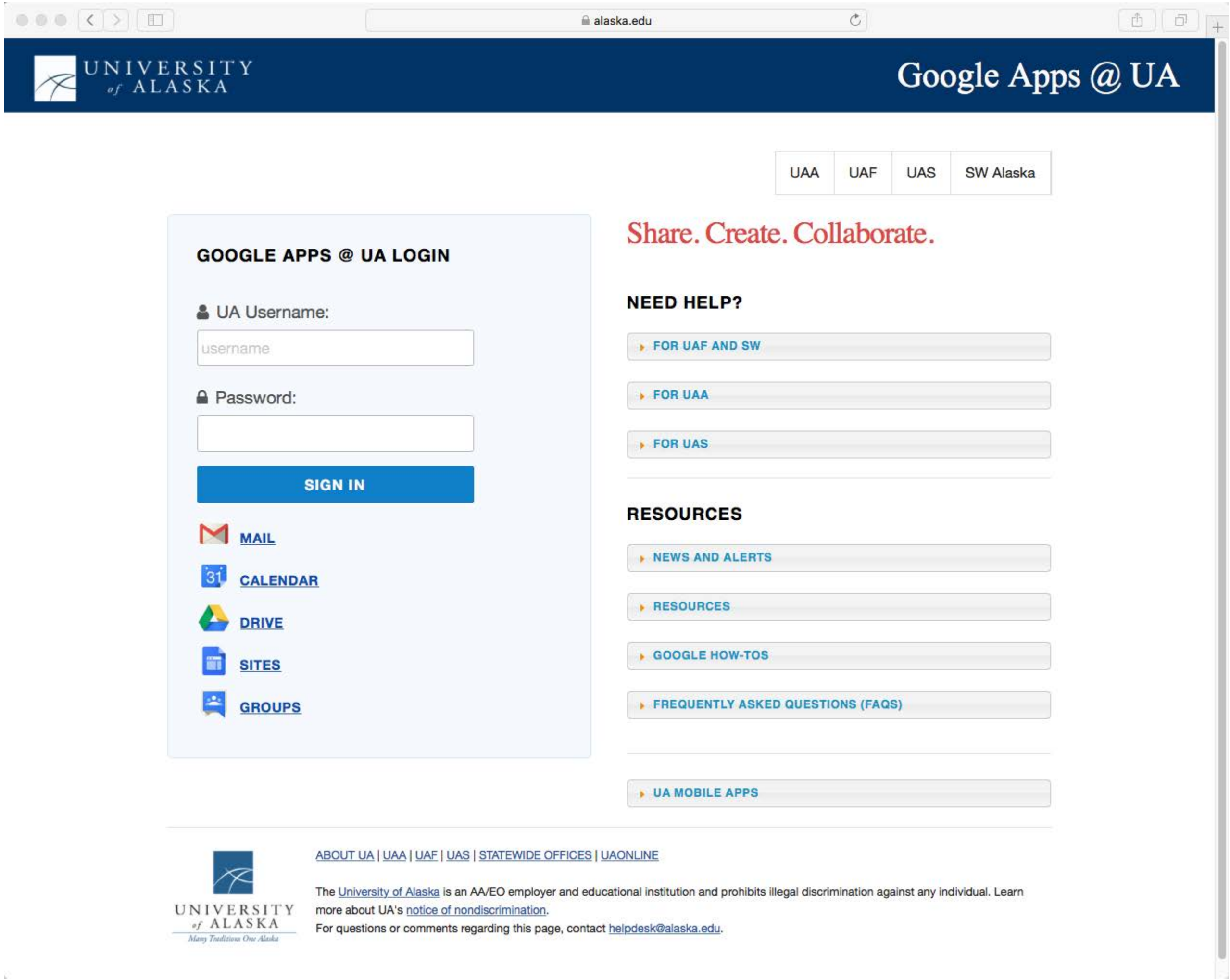


We do not ask for both Username & Email

Confirm the password on a login screen?!

Learn what is normal and question anything that does not fit that expectation.

Ours



alaska.edu

UNIVERSITY of ALASKA

Google Apps @ UA

UAA | UAF | UAS | SW Alaska

GOOGLE APPS @ UA LOGIN

UA Username:

username

Password:

SIGN IN

MAIL

CALENDAR

DRIVE

SITES

GROUPS

Share. Create. Collaborate.

NEED HELP?

- FOR UAF AND SW
- FOR UAA
- FOR UAS

RESOURCES

- NEWS AND ALERTS
- RESOURCES
- GOOGLE HOW-TOS
- FREQUENTLY ASKED QUESTIONS (FAQS)

- UA MOBILE APPS

UNIVERSITY of ALASKA
Many Traditions One Alaska

ABOUT UA | UAA | UAF | UAS | STATEWIDE OFFICES | UAONLINE

The University of Alaska is an AA/EO employer and educational institution and prohibits illegal discrimination against any individual. Learn more about UA's notice of nondiscrimination.
For questions or comments regarding this page, contact helpdesk@alaska.edu.

What are some of the places I should be cautious?

Person to Person sales apps & sites

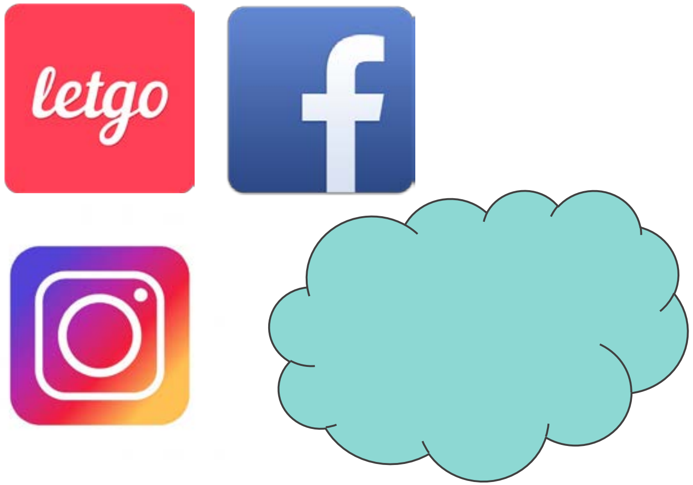
The cloud

Social media

Public wifi networks

Online “Canadian” Pharmacies

Bank of the Western Islands US Territory and Truck Sales websites



Not social engineering attacks...

Malware - software meant to steal information or resources

MIIM - unsecure or untrusted networks can let 3rd parties have access to your information on the network

APT - an automated attack that is always on, searching for a target and can evade detection

Physical theft - most often involves mobile devices but when we connect those devices to information services (email, facebook) they become portals to useful data to an attacker

Dumpster diving - those passwords you wrote down but did not lock up or shred, the tax form you just put out with the trash

What about while I am at work or doing University business?

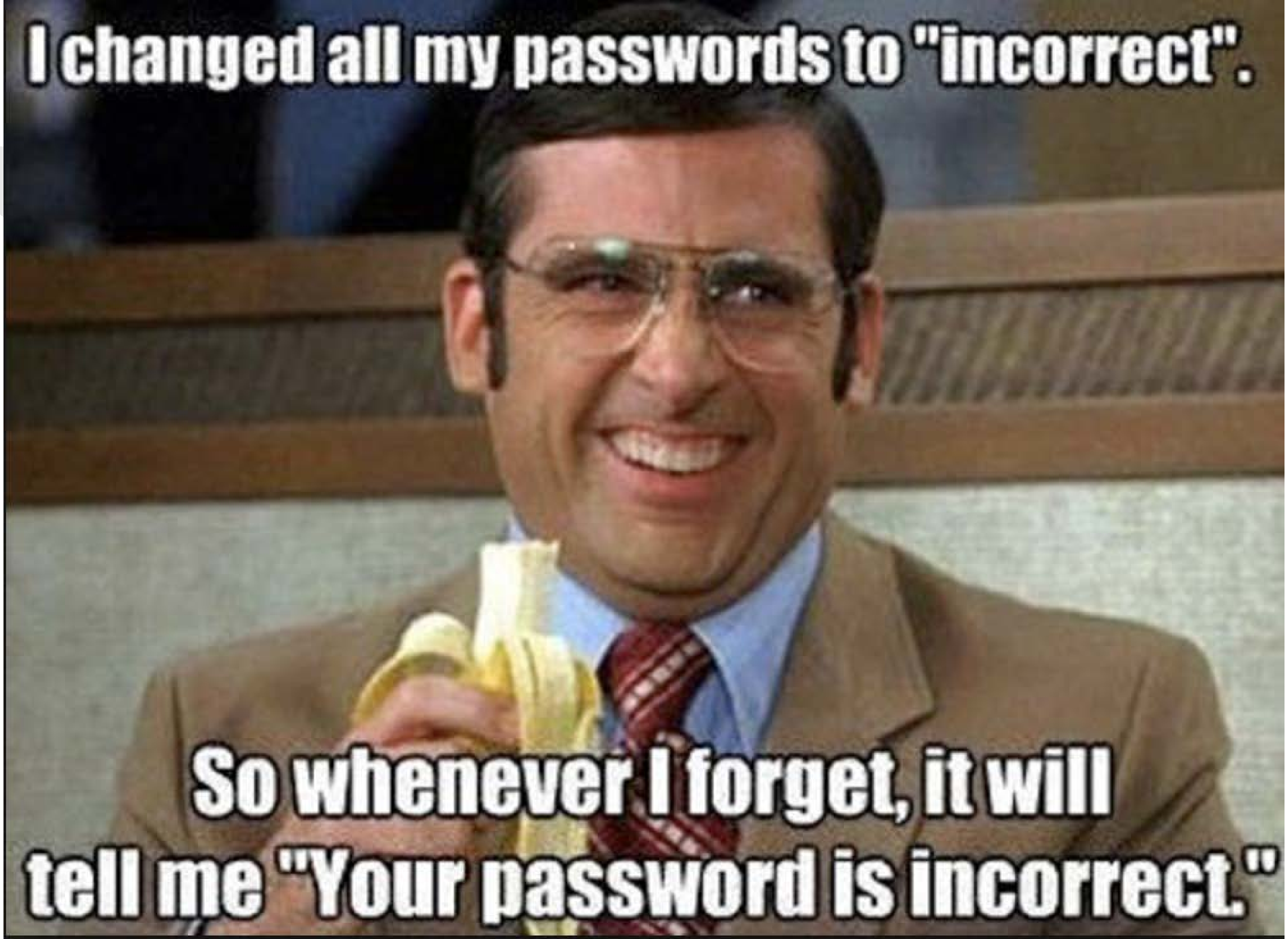
All the same advice applies equally - the risk is higher in the workplace

Unique scams and threats you can expect in the office:

- CEO fraud (aka wire fraud)
- W2 solicitation
- Direct deposit fraud
- Identity information theft
- Resource theft
- Denial of Service (DoS)

What can I do to keep myself, my family, my coworkers, students and the University safe!?

1. Stop. Think. Connect. (https://www.stopthinkconnect.org/)
2. Keep operating systems and software up to date
3. Have and keep anti-virus software up to date
4. Us secured, trusted networks to work from
5. Use good passwords & go ahead and write them down
6. For mobile devices enable location tracking, device encryption and remote wipe features
7. Learn what normal is and ask questions when something does not look right


I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

Keep a Clean Machine

- **Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that’s an available option.
- **Protect all devices that connect to the Internet:** Along with computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information

- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

- **Make your password a sentence:** A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, “I love country music.”). On many sites, you can even use spaces!

- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.

- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that’s stored in a safe, secure place away from your computer. You can alternatively use a service like a password manager to keep track of your passwords.

Connect With Care

- **When in doubt, throw it out:** Links in emails, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- **Protect your $$:** When banking and shopping, check to be sure the site is security enabled. Look for web addresses with “https://” or “shttp://,” which means the site takes extra measures to help secure your information. “Http://” is not secure.

Be Web Wise

- **Stay current.** Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.
- **Back it up:** Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen

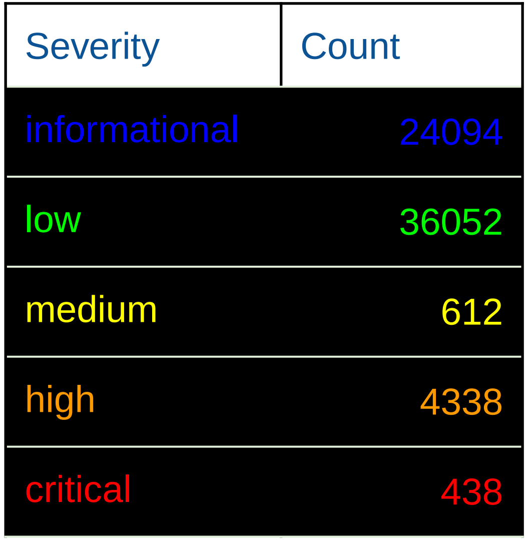
- **Safer for me, more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you.** The Golden Rule applies online as well.
- **Help the authorities fight cybercrime:** Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.

Own Your Online Presents

- **Personal information is like money. Value it. Protect it.:** Information about you, such as your purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it’s collected through apps and websites.
- **Be aware of what’s being shared:** Set the privacy and security settings on web services and devices to your comfort level for information sharing. It’s OK to limit how and with whom you share information.
- **Share with care:** Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it could be perceived now and in the future.

So what does OIT do to keep us safe?

1. OIT manages workstations and some software.
2. OIT operates managed anti-virus software.
3. OIT maintains visibility of sensitive information.
4. OIT operates intrusion detection and prevention systems.
5. OIT maintains logs of activity to determine when and how an incident might have taken place, or not.

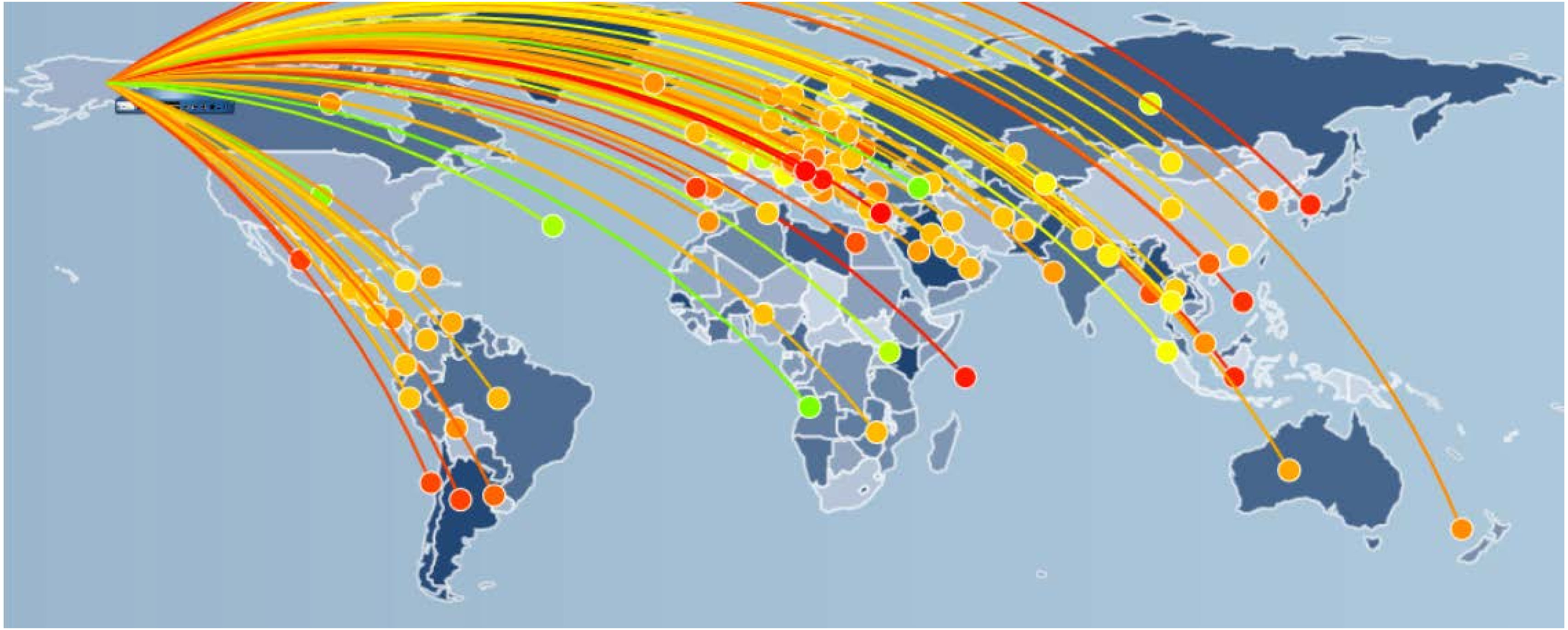


Severity	Count
informational	24094
low	36052
medium	612
high	4338
critical	438

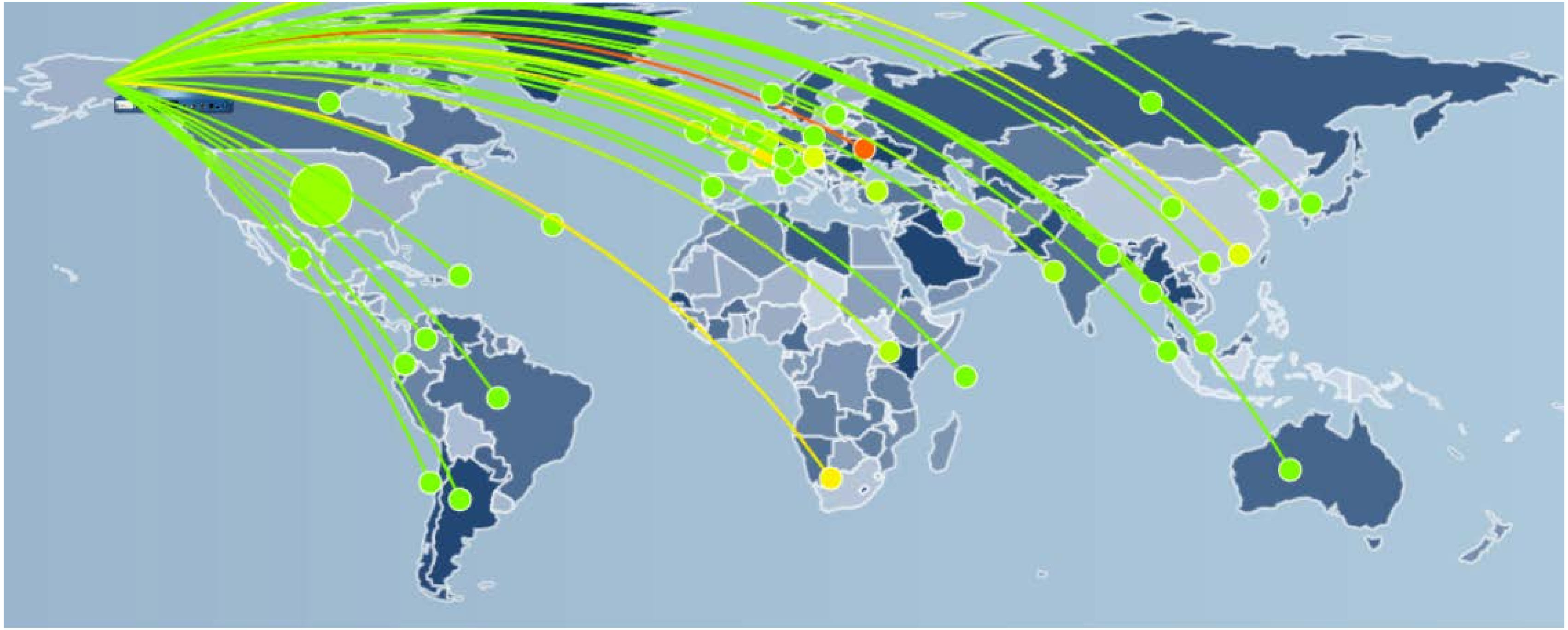
4,776 high/critical events per day x 365 days = 1.7 million per year

It costs ~$0.21 per denied high/critical threat based on our current volume.

Top 100 incoming threats in the last 24 hours.



Top 100 Outgoing Threats in the last 24 hours



Questions