



Nutella 
@NutellaGlobal

Follow



Today it's World Password Day: choose a word that's already in your heart. Like "Nutella", for example! #WorldPasswordDay #Nutella



“

**A real Nutella® Lover
never forgets his
password.**


”



Equifax reveals full horror of that monstrous cyber-heist of its servers

146 million people, 99 million addresses, 209,000 payment cards, 38,000 drivers' licenses and 3,200 passports

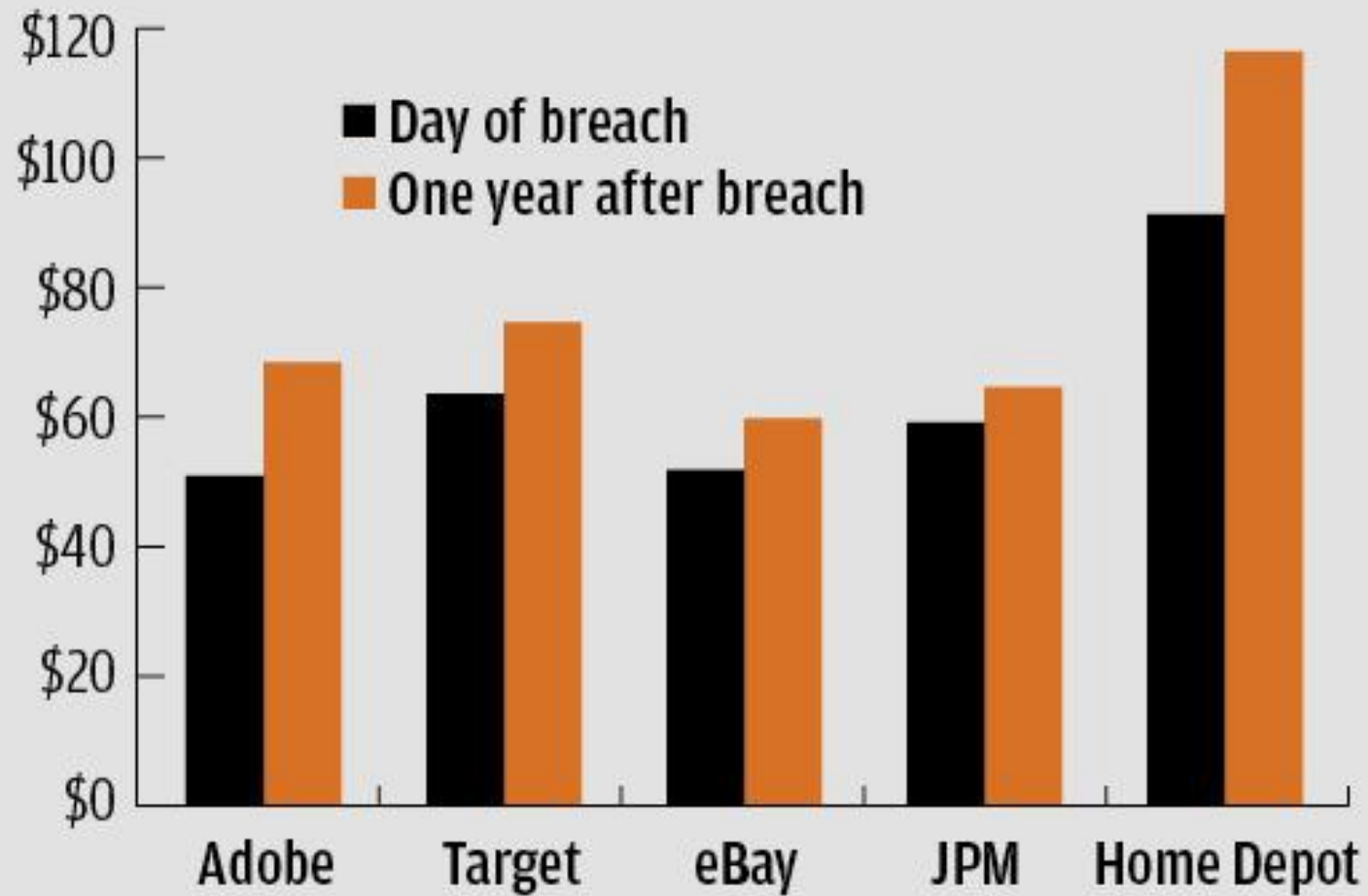
By [Richard Chirgwin](#) 8 May 2018 at 02:57

48  SHARE ▼

Equifax has published yet more details on the personal records and sensitive information stolen by miscreants after they hacked its databases in 2017.



Per share price after data breaches



Mar 1, 2018 | Avi Mizrahi | 👁 5002 💬 21 Comments

Louisiana Attorney General Fires IT Staff for Allegedly Mining Bitcoin

It appears that the allure of free electricity and computer systems, courtesy of the tax payers, might be too hard for some government workers all over the world to resist. After it was recently revealed that Russian nuclear scientists were arrested for mining bitcoin on the job, now it is reported that American IT staff apparently lost their jobs for doing the same in Louisiana.



Florida State Employee Arrested for Allegedly Mining Crypto at Work

GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry

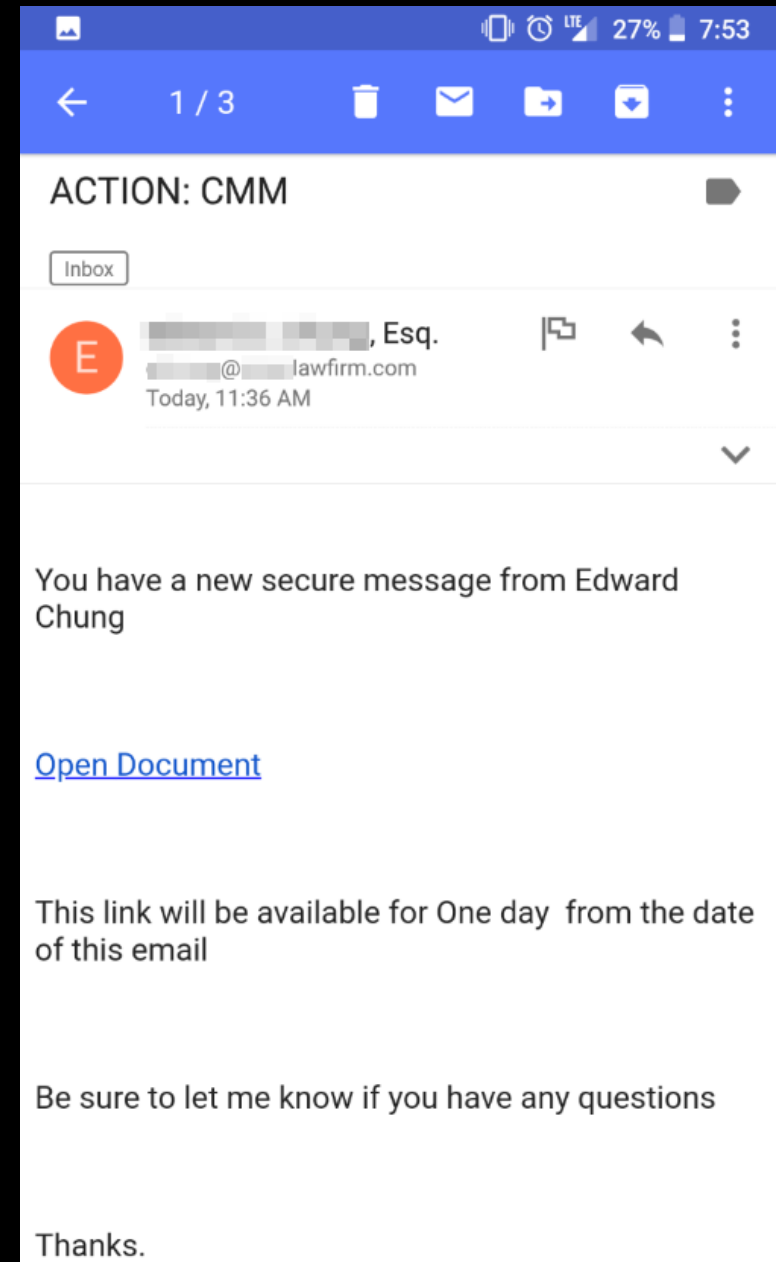
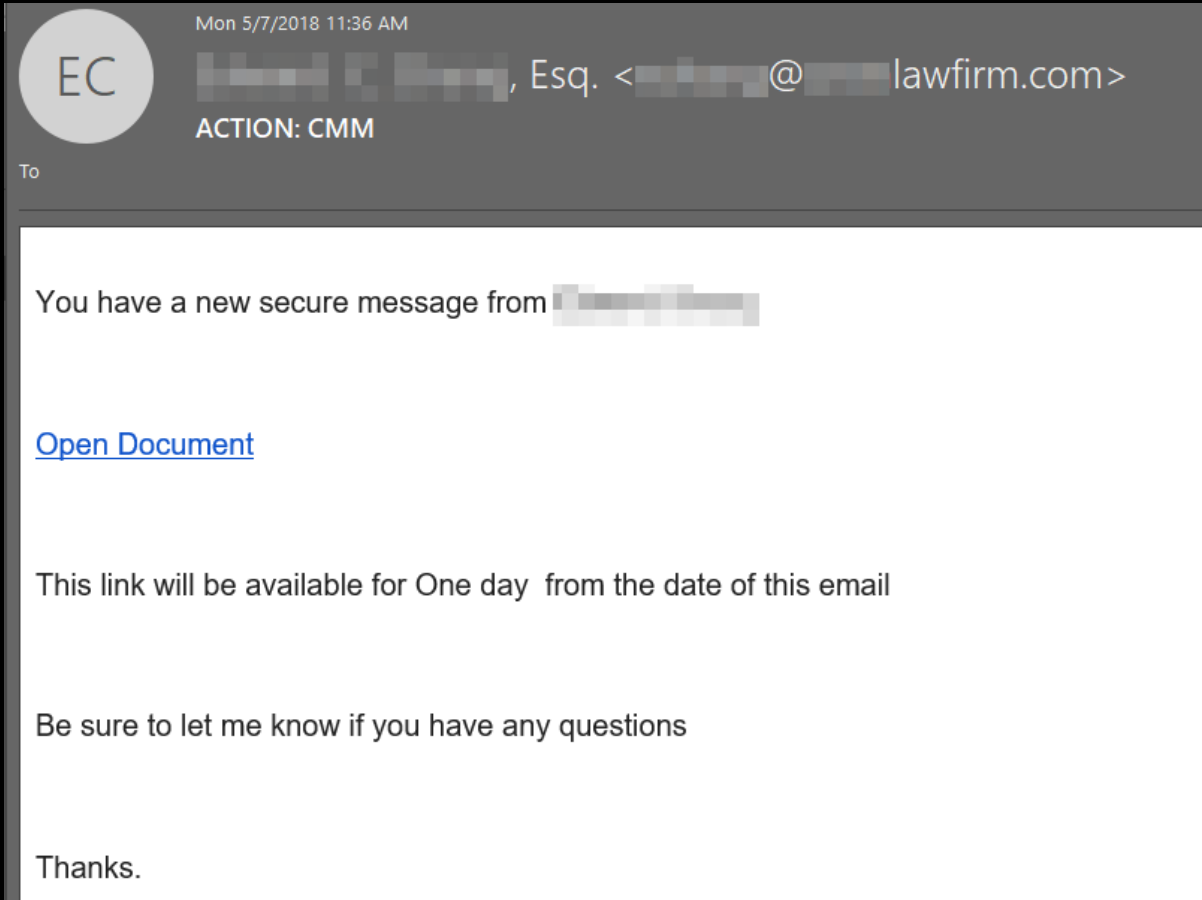
WEDNESDAY, APRIL 18, 2018

BY: COUNTER THREAT UNIT RESEARCH TEAM

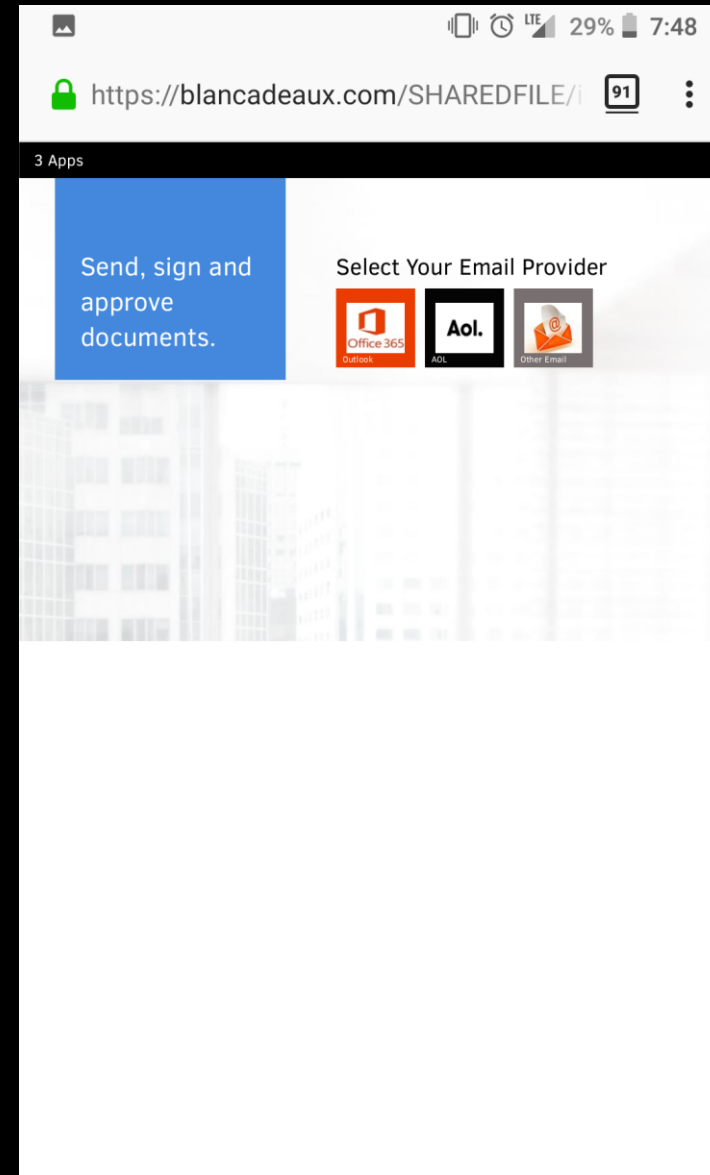
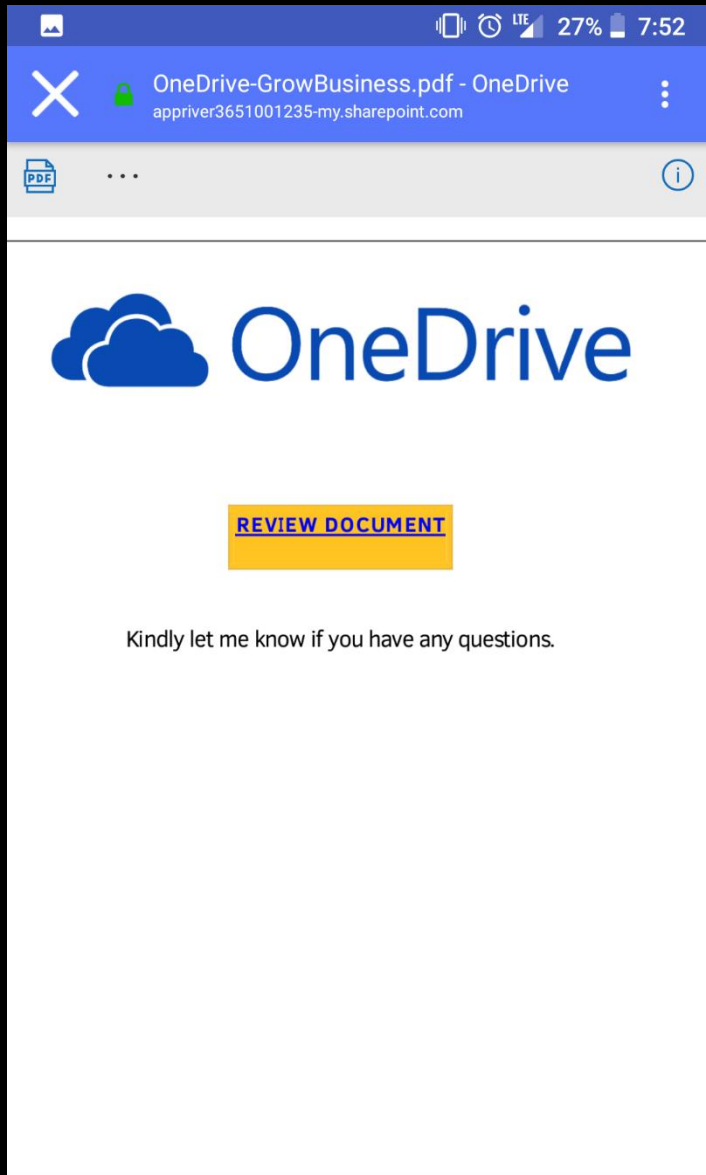


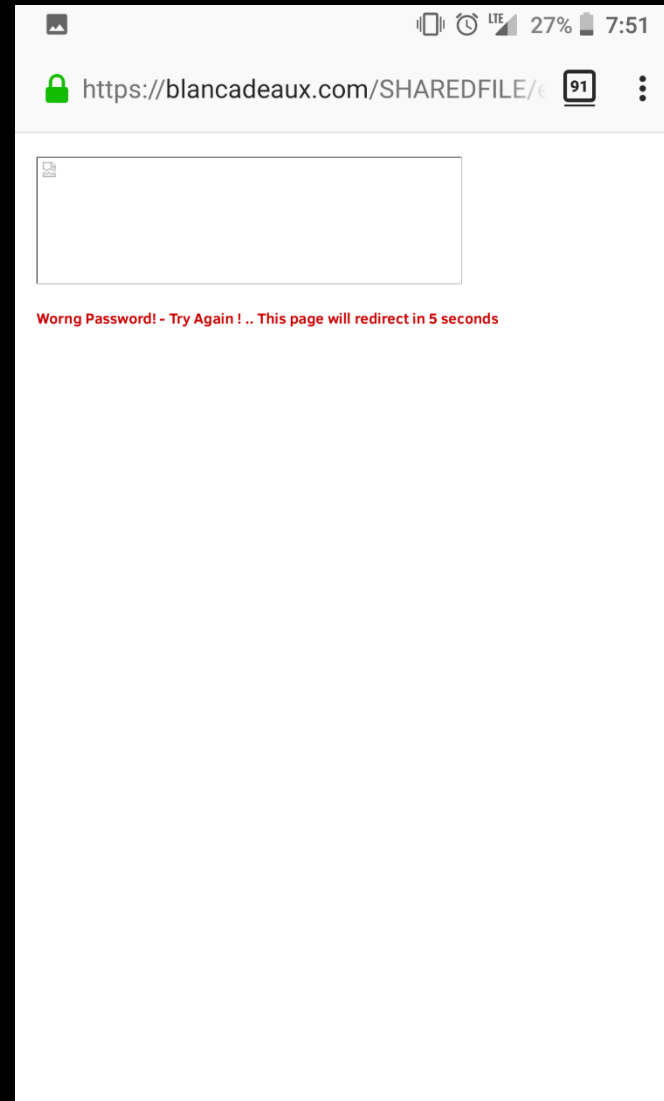
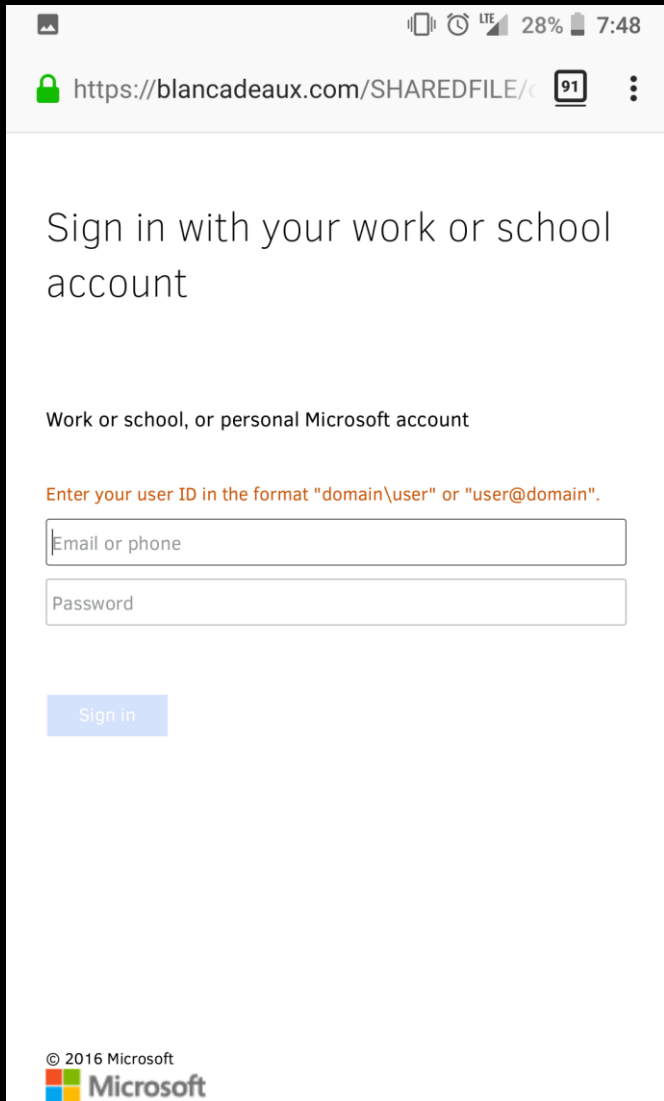
Summary

In 2017, Secureworks® Counter Threat Unit™ (CTU) researchers continued to track GOLD SKYLINE, a financially motivated Nigerian threat group involved in business email compromise (BEC) and business email spoofing (BES) fraud. During the investigation, CTU™ researchers discovered a previously unidentified BEC group that they have named GOLD GALLEON.



<https://appriver3651001235-my.sharepoint.com/personal/██████████-██████████law.com/layouts/15/guestaccess.aspx?e=jujeQ5&share=EV8BFrsRslHir7rsn-maUBFI9FbEB51UbeHWnJJ3ZPVQ>







Mon 5/7/2018 4:12 PM

IT DEPARTMENT <IT@[REDACTED]lawfirm.com>

(RESOLVED) PHISHING NOTICE TO RECIPIENT OF EMAIL ENTITLED: ACTION: CMM

To IT DEPARTMENT

Dear Recipient of Email Entitled: ACTION: CMM

On Monday, May 7, 2018, it came to our attention that an email ([REDACTED]lawfirm.com) belonging to the Senior Partner of [REDACTED], PLLC as well as a number of emails of other local law firms that use Office 365 were being sent out as part of an attempted phishing hack.

YOU ARE HEREBY ADVISED THAT THIS IS NOT A LEGITIMATE CORRESPONDENCE FROM [REDACTED], PLLC AND YOU SHOULD NOT OPEN OR ATTEMPT TO OPEN THE EMAIL ENTITLED: ACTION CMM.

WE HAVE BEEN ADVISED BY MICROSOFT THAT IF YOU OPEN THIS EMAIL IT WILL ATTEMPT TO MANAGE YOUR RULE SETTINGS ON OUTLOOK WHEREIN ANY EMAILS COMING IN OR BEING SENT OUT WILL BE SENT TO YOUR DELETED INBOX. MICROSOFT HAS BEEN PUT ON NOTICE AND HAS CORRECTED THE ISSUE BY DELETING THIS RULE; HOWEVER, OUT OF AN PRECAUTIONARY MEASURE YOU ARE ADVISED TO CHECK YOUR RULE SETTING TO ASSURE THAT THIS RULE HAS NOT BEEN IMPLEMENTED ON YOUR EMAIL. PLEASE BE ADVISED THAT MICROSOFT'S SOLUTION FOR RESOLVING THIS ISSUE WAS TO CHECK YOUR RULES ON OUTLOOK AND DELETE ANY RULE THAT YOU DID NOT SET.

At this time, there is no indication that there was any acquisition of any sensitive personal data or information. Nevertheless, we are sending you this courtesy notice to check your email rule setting as a precautionary measure based on what we were advised by Microsoft.

IT Department



Confidentiality Notice: This email message and any other information attached to this email is for the sole use of the named addressee and may contain, privileged and confidential information which may be protected from disclosure. If you believe that it has been sent to you in error, you may not read, disclose print, copy, and store or disseminate the e-mail or any



ILLINOIS.GOV

Microsoft Outlook Webmail

Select Agency

Domain\user name:

Password:

[➔ sign in](#)

Microsoft Excel

Sign in with your valid email account to view document.


Email Address

Email Password

CONTINUE

Privacy policy
personal information will be not disclosed or accessed by a third party. Applicable to unregistered users.

Microsoft excel ©2017





Work or school account

someone@example.com

Password

Keep me signed in

Sign in



Have You Ever

- Clicked “I forgot my password” and had the actual password delivered to your inbox?
- Been asked for your mother’s maiden name, high school mascot, best childhood friend, or favorite author as a password reset question?
- Had an IT administrator that knew your password?
- Used the same password at work as you do for your personal accounts?



Safe(r) Computing

Agenda

- What is the problem?
- Identifying the most common threats.
- Steps to take to protect yourself and others.
- Q&A



So What is the Problem?

How we got here.

Threat Evolution

- Global, persistent hyper-connectivity
- Inexpensive and highly available computing
- Internet Freedom

Know Your Adversaries

They want money!!!

- Data
- Cash
- Intellectual Property
- Revenge
- Power
- Influence

Know **Their** Rules

They don't care about your ethics

They don't care about your laws

They don't care about your family

They don't care about your business

They don't care about your morals

They don't care about you

They don't sleep

“Bad actors have quotas too”

Why is **security** hard?

- We like helping
- We don't want to be "that person"
- We are trusting
- We are lazy
- We are fallible
- We are in different stations in life
- We have diverse morals

Immutable Laws of Security

Law #1: If a bad guy can persuade you to run his program on your computer, it's **not solely your computer anymore**.

Law #2: If a bad guy can alter the operating system on your computer, it's **not your computer anymore**.

Law #3: If a bad guy has unrestricted physical access to your computer, it's **not your computer anymore**.

Law #4: If you allow a bad guy to run active content in your website, it's **not your website any more**.

Law #5: **Weak passwords trump strong security**.

Law #6: A computer is only as secure as the **administrator is trustworthy**.

Law #7: Encrypted data is only as secure as its decryption key.

Law #8: An out-of-date antimalware scanner is **only marginally better than no scanner at all**.

Law #9: Absolute anonymity isn't practically achievable, online or offline.

Law #10: **Technology is not a panacea**.

Source: [The 10 Immutable Laws of Security](#)

A person wearing a dark hoodie is shown in profile, looking down. The lighting is dramatic, with the person's face and the texture of the hoodie partially illuminated against a dark background. The overall mood is mysterious and somber.

Identifying Common Threats

The Goal: Stop Clicking on Everything

Not Going to Cover

Drops

- If you find a thumb drive, receive one at a conference, or just happen upon one, **DON'T plug it in**

Remote Connectivity

- Just because it says "Free Wifi", "Conference Wifi", "Google Internet", don't use it

Website

- Vulnerability in your company website; you paid a lot for it, who maintains it's security?

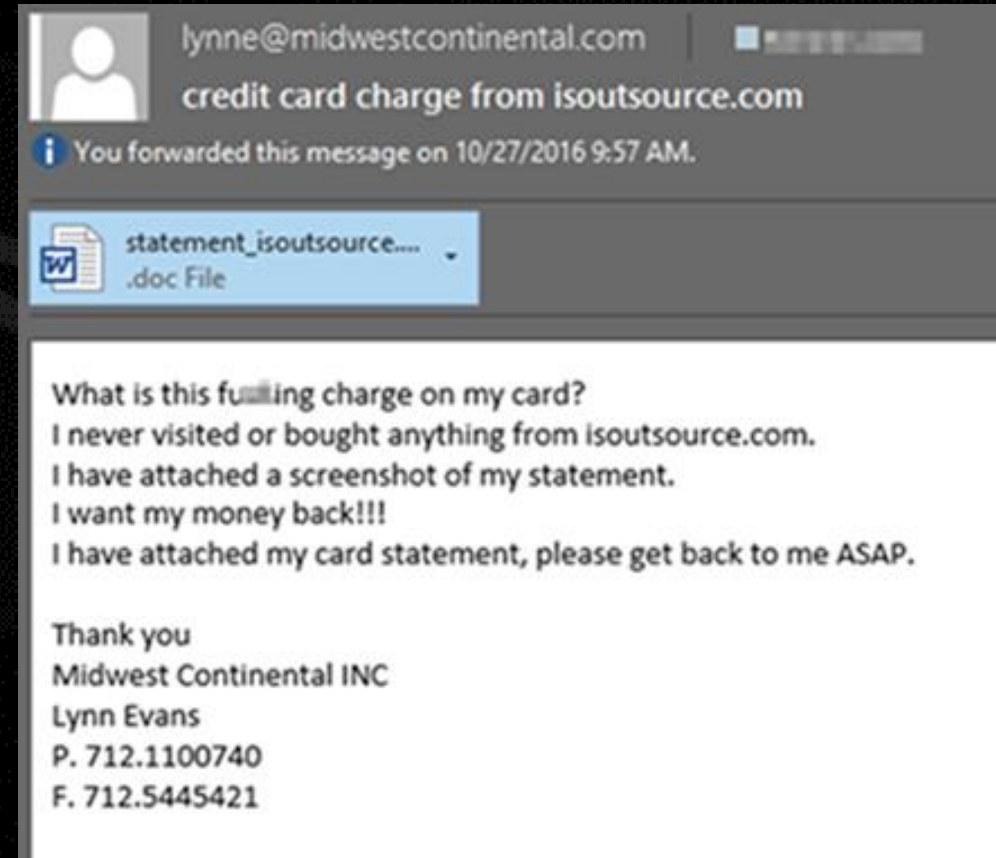
Example: RansomWare

- Ransom: All your data
- Indiscriminate
- Mitigation:
 - Backups, Tested and Verified Regularly
 - Training
 - Strong, multi-layered protections and access controls
- Losses: ++\$1 billion/year



Example: Social Engineering

- Typically multi-faceted: Phone, Email, SMS
- Timespan can be days to years
- Most modern attacks use some form of social engineering
- Mitigation:
 - Personnel training
 - Physical controls
 - Role based access controls



Example: Phishing (+ Spear Phishing)

- Masquerades as trustworthy source
- Usually email but can be phone, mail
- Targeted (spear phishing > phishing)
- #1 source for phishing leads:
 - Social Media (LinkedIn+++, Facebook)
- Mitigation:
 - Multi-Layer Defense
 - Role based access controls
- Losses: ~\$3-5 billion/year

Mail from: victoriaj@widgetcorp.com

Diane,

We just closed a deal with a brand new vendor and I need you to do a quick transfer to close. Let me know when you get this and I'll shoot you over the account and routing details. I'm on a call for the next couple hours but if you text me, I'll confirm the transaction.

This is great news for our company! Thanks for your help and hard work.

Victoria Johnson

victoriaj@widgetcorp.com

Chief Financial Officer | Widget International Corp.

(p) (425) 555-8809 | (c) (206) 555-2309 | (f) (425) 555-8800

Correct Signature:

Victoria Johnson

victoriaj@widgetcorp.com

Chief Financial Officer | Widget International Corp.

(p) (425) 555-8509 | (c) (206) 555-2809 | (f) (425) 555-8500



Bluehost abuse12@bluehost.com via annika.timeweb.ru

7:38 AM (1 hour ago) ☆



to me ▾

Dear Bluehost customer [REDACTED]

It has come to our attention that your site is using an excessive amount of MySQL resources on your BlueHost.Com account. This is causing performance problems on your website as well as for other customers that are on this server. It can cause our servers to crash and cause additional downtime.

Our research shows that server performance degrades when the MySQL usage is over 1,000 tables and/or 3 GB on a single account or 1,000 tables and/or 2 GB on a single database. In order to ensure optimal performance for your account and the others in your shared hosting environment, we request that you reduce the MySQL usage on your account to under these limits in 14 days.

You must confirm the current copy of our Terms of Service here:

[http://my.bluehost.com.75a7e9d83024b7ce00fe9cd2aa0bd0c5.h116122.s23.test-hf.su/
domain/\[REDACTED\]](http://my.bluehost.com.75a7e9d83024b7ce00fe9cd2aa0bd0c5.h116122.s23.test-hf.su/domain/[REDACTED])

How to fix:

[http://mysql.bluehost.com.75a7e9d83024b7ce00fe9cd2aa0bd0c5.h116122.s23.test-hf.su/
domain/\[REDACTED\]](http://mysql.bluehost.com.75a7e9d83024b7ce00fe9cd2aa0bd0c5.h116122.s23.test-hf.su/domain/[REDACTED])

Terms of Service Compliance Department

1958 South 950 East

Provo, UT 84606

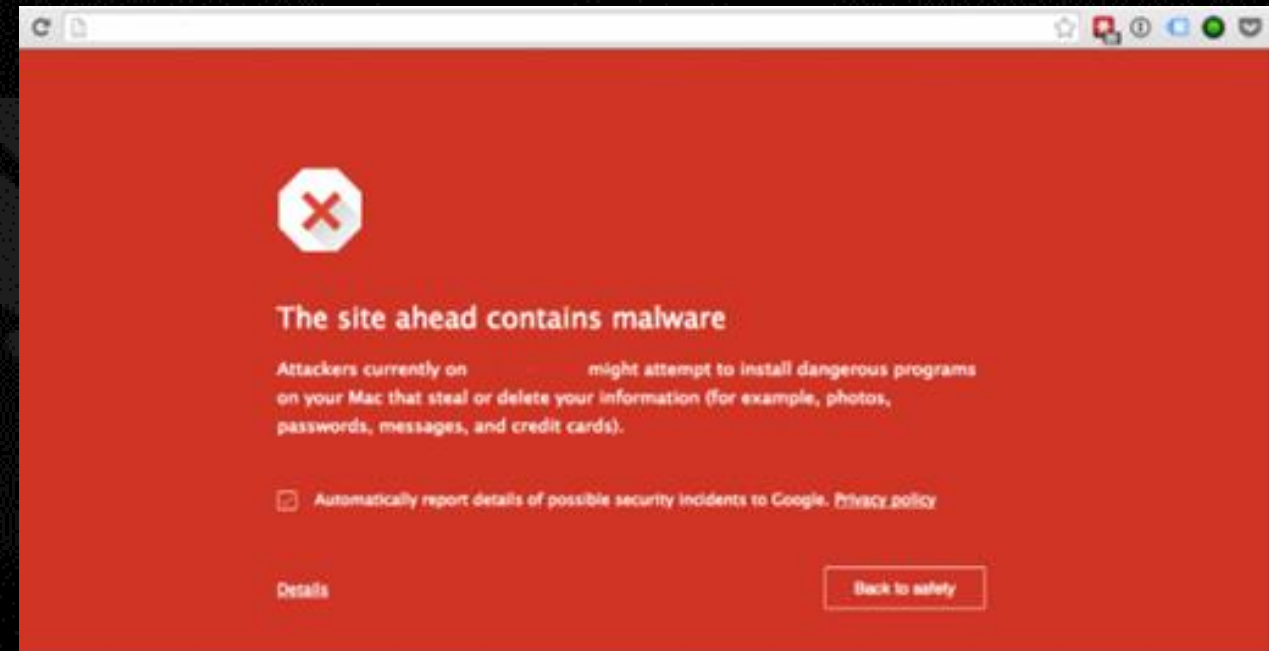
Phone line: (888) 401-HOST Option 5 | Fax line: [801-765-1992](tel:801-765-1992)

Example: Wire Fraud

- Typically targeted and heavy with social engineering techniques
- Can be highly sophisticated
- Typically includes only hand selected financial personnel within an org
- Mitigation:
 - Training + Policy for all staff w/ wire authority
 - Check all email headers (see resources) and require callback with authentication for all transactions.
 - Callbacks must require verification and authentication
 - Policies should require this level of integrity and authenticity.
 - Minimum of two person integrity is preferred for all transactions

Example: Website Hack

- What is the value of your website? Your reputation?
 - Hijacked with malware?
 - Denial of Service/Availability?
 - Brand identity / trustworthiness?
 - Sales and Marketing losses?



Example: (Bit)coin Mining

- Mining is unprofitable unless you can steal electricity and/or computing resources
- Ransomware single handedly changed how the industry thought about security
- Cryptocurrency mining is mostly ignored



Your Defense

People Are The Perimeter



- Personal Devices
- Social Media
- Hyper-Connectivity
- There are **no** patches for this vulnerability

People Strategy

- Train and Assess Security IQ
- Require credit and background screenings as part of standard employment
- Business should encourage safe practices regarding passwords
 - Recommend purchasing 'password management' software for employees
- Vet all personnel and 3rd parties with access to your data as you would a member of executive staff.
 - Often the same level of access (sometimes more).

Backup Strategy

- Backups must be tested and verified regularly
- Automate your backups
- Remove the human factor
- Store offsite and not connected to production
- Common things missed:
 - Are backups secured?
 - Device Configurations
 - Desktops and Mobile Devices

Culture Strategy

- Embrace healthy skepticism
 - Create a “better safe than sorry” environment
 - “See something, say something”
- Policies and procedures must provide:
 - Safe reporting
 - Full participation of all

Update Your Systems

- Once I trick you, I look for vulnerable systems (pivot)
- If I can't trick you, I look for vulnerable systems
- If I don't want to deal with you, I look for vulnerable systems
- If I'm bored, I look for vulnerable systems
- If I don't have time, I automate my search for vulnerable systems

Update Strategy

- Establish and maintain a hardware and software portfolio
- Establish a regular patch schedule (min. Monthly)
- Automate patching and updating
- Plan for and execute on out of band and critical patches released by vendors
- Don't neglect switches, firewalls, and IoT devices, Your Website!

If I had your password, I would...

- Try that password
 - against your bank, personal email, Amazon, Facebook, Netflix, LinkedIn, etc.
- If I get access to your email, I can and will reset all your passwords
- If I'm on your network, it's not your network anymore.

Password Strategy

- **Do:** store your passwords in a password safe (e.g. lastpass, dashlane)
- **Do:** use a different password for everything. It's especially easy when you have a secure way of storing it. See above.
- **Do:** long passwords trump complex passwords.
 - **Good:** 18Puppies&18Unicorns
 - **Bad:** Unicorns!
- **Do:** avoid things that are easy for me to guess like your middle name or your spouse's name or your kid's name or your dog's name...
- **Do:** enable two factor authentication

Passwords Are Like Underwear

You shouldn't leave them lying around

You should change them often

It's best if you don't share them with friends

Don't leave them out for others to see

Recommendations

- Automate the backup of your data
- Learn to identify online threats. Practice!
- Establish security protocols in the office and at home
- Use updated and modern AV & Malware protection
- Block all non-required traffic, in and out (uBlock Origin, OpenDNS®, Firewall)
- Use a Password Vault and Two Factor Authentication

Home Checklist

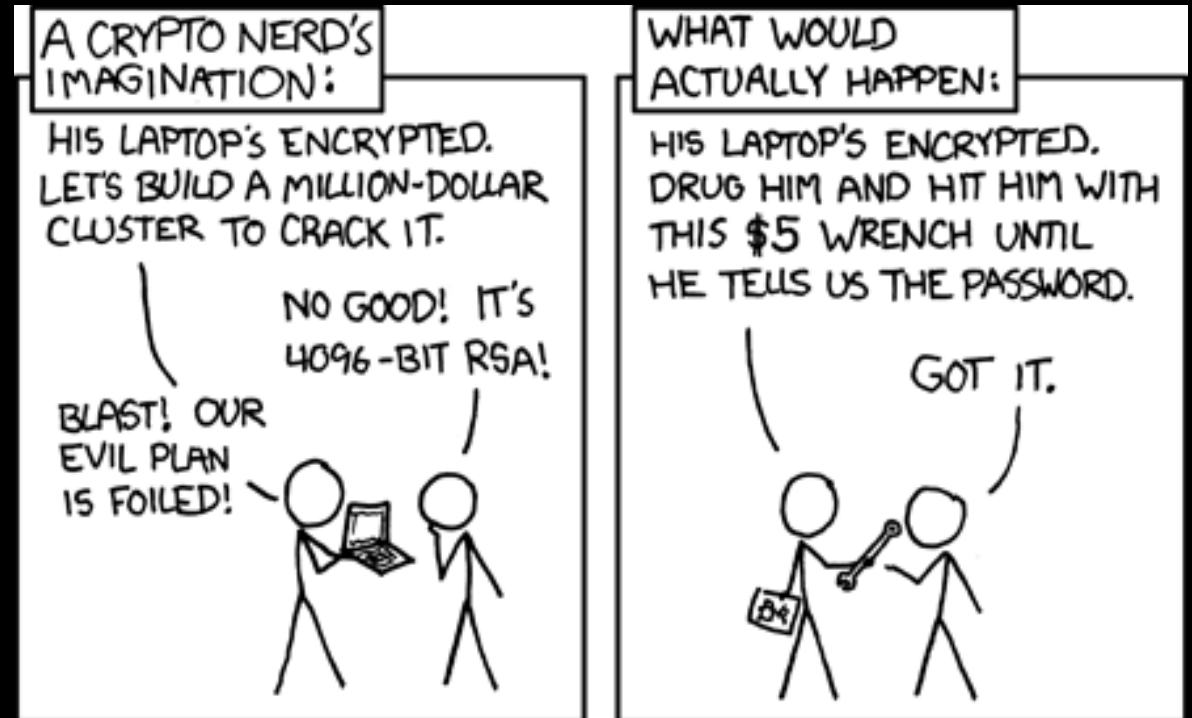
- Automate your backups
- Uninstall unnecessary programs
- Enable automatic updates
- Use a password manager and do not reuse passwords
- Setup two factor authentication on banking, email, social media, and credit related sites
- Update home router and firewall firmware
- Change default passwords on all devices (cameras, DVR, firewall)
- Use an Adblocker (Ublock Origin)

Business Checklist

- Inventory all hardware and software
- Automate and test onsite and offsite backups
- Build secure standards for desktops, mobile devices, and servers
- Continuously assess and remediate internal and external vulnerabilities
- Reduce all use of administrative rights
- Monitor and maintain logs on all systems
- Limit and control both incoming and outgoing network traffic

Q & A

Safe(r) Computing



Contact Info:

Andrew Healey

andrewh@isoutsource.com

<https://www.linkedin.com/in/andrewhealey>

ISOutsource

www.isoutsource.com

(800) 240-2821