FERPA Considerations:

Data Security

Arkansas Department of Higher Education

March 12, 2018

Mike Tassey
Privacy Technical Assistance Center

FERPA & Data Security

What specific technology controls does FERPA require for your IT systems?

FERPA & Data Security

Yup… Nada… Nothing… Zilch…

FERPA & Data Security

Why doesn't FERPA tell me **how** to protect student records?

FERPA & Data Security

- FERPA was written in 1974…
- Initially focused on the protection of paper records and information.
- This is both a blessing and a curse.
- FERPA deals addresses data security through the concept of “Reasonable Methods”

FERPA & Data Security

rea·son·a·ble meth·od

/ˈrēz(ə)nəb(ə)l/ /ˈmeTHəd/

We generally interpret reasonable methods to mean a set of security controls that are in line with current accepted security and privacy best practices for data of similar sensitivity.

FERPA & Data Security

≠

Cyber Budget = Gym Teacher

Cyber budget = $6.7 Billion

FERPA & Data Security

- Technology

- Policies

- Training

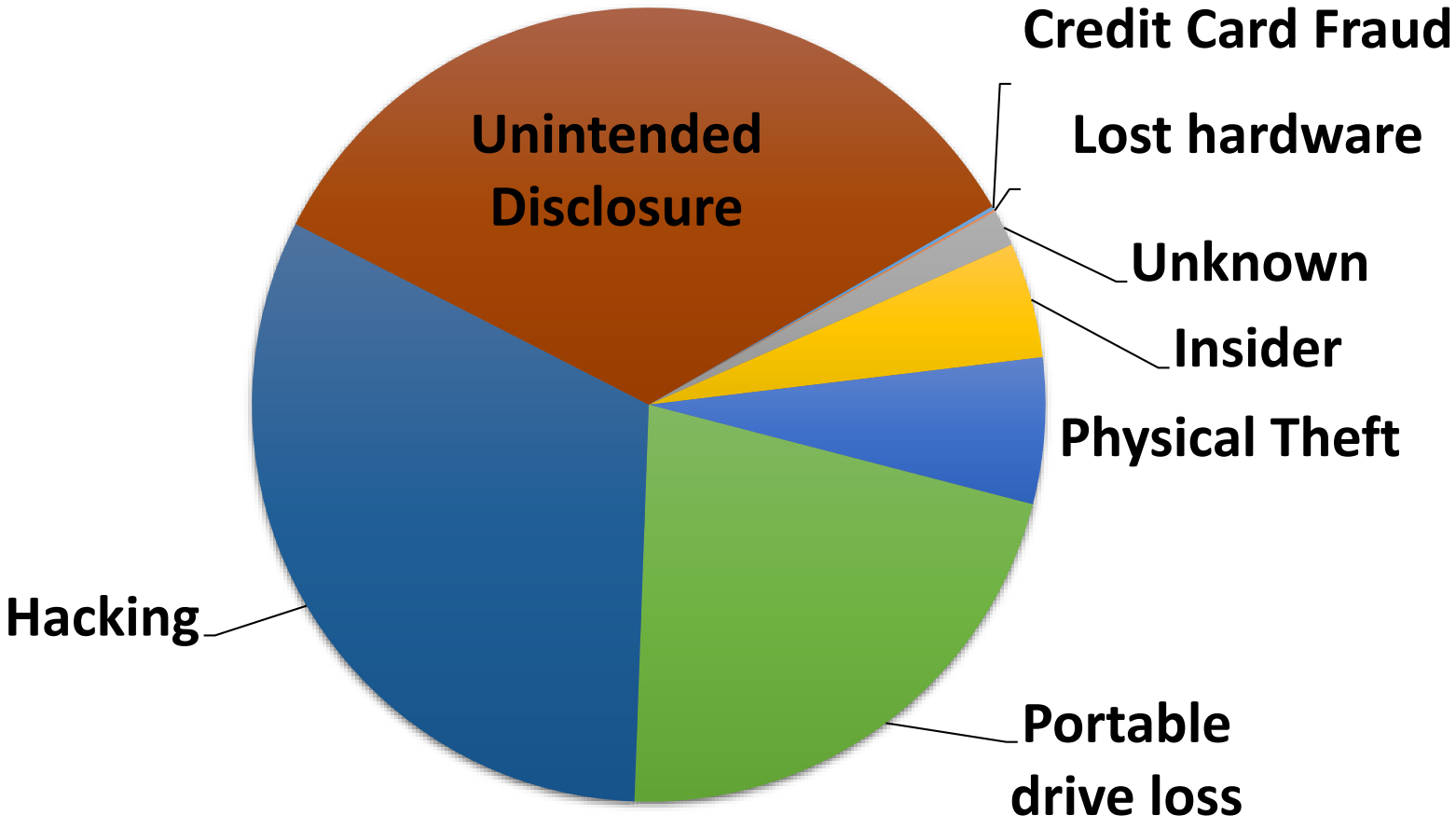
Data Security - Why

- FERPA requires it.
- Students deserve it.
- A breach could cause reputational harm.
- Electronic records are more prevalent than ever.
- We collect more, move more, use more & lose more data than ever before.

The Facts - 2017

- Over 100 data security incidents
- >1.1 Million records breached
- > 3,000 records per day
- Loss includes:
  - *SSN*
  - *Names*
  - *Addresses*
  - *Grades*
  - *Emails*
  - *Employee data*
  - *Discipline records*
  - *Tax data*

The Causes


Credit Card Fraud
Lost hardware
Unintended Disclosure
Unknown
Insider
Physical Theft
Hacking
Portable drive loss

The Facts - 2018

California College of the Arts CA
Wallace Community College Selma AL
University of Wisconsin - Superior WI
Thomas Edison State University NJ
Midland School District IA
Livingston County Schools KY
Mississippi State University MS
Saginaw Valley State University MI
San Diego County Office of Education CA
Monticello Central School District NY
Broward College FL
Oklahoma State University Center for Health Sciences OK
Columbia Falls School District MT
Montana State University Billings MT

331,512 Records

AR Map

FERPA & Data Security

- "Secure" doesn't exist
- Data security is all about managing risk
- No one is 100% patched
- Nobody can predict the 0-day attack

Problems in ED Data Systems

- A ton of old or unpatched software
- IoT devices in schools include:
  - Server room cameras & sensors
  - School surveillance systems
  - Access card readers
  - Modems (UPnP hackable)
  - HVAC / Boilers
- Hundreds of forgotten servers / computers

Problems in ED Data Systems for one state found in an afternoon!

- 626 machines with no firewall
- 2 SIS breaches affecting thousands of students
- Hundreds of anonymous FTP servers
- 143 Windows XP machines (some already compromised)
- 10 VPNs running out of date Windows 2003 Server
- 835 Web servers running IIS 6 or earlier

Why me?

a hacker's best friend:

OK Google…. Find me some passwords

TOTAL RESULTS

12

TOP COUNTRIES

United States	12

TOP SERVICES

HTTP	8
HTTPS	4

Let's "switch" it up…

23
tcp
telnet

```
---------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15.

YOU MUST USE CISCO CP or the CISCO IOS CLI TO CHANGE THESE  PUBLICLY-KNOWN
CREDENTIALS

Here are the Cisco IOS commands.

username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco

Replace <myuser> and <mypassword> with the username and password you want
to use.

IF YOU DO NOT CHANGE THE PUBLICLY-KNOWN CREDENTIALS, YOU WILL NOT BE ABLE
TO LOG INTO THE DEVICE AGAIN AFTER YOU HAVE LOGGED OFF.

For more information about Cisco CP please follow the instructions in the
QUICK START GUIDE for your router or go to http://www.cisco.com/go/ciscocp
---------------------------------------------------------------------


User Access Verification

Username:
```

5.5.49-0ubuntu0.14.04.1

Out of Date-a-bases

5.1.52-community
5.0.26
5.1.49-community
5.5.49-0ubuntu0.14.04.1
5.5.56-MariaDB
5.5.36-log

TOTAL RESULTS

10

TOP COUNTRIES

United States 10

1	CVE-2016-7478		DoS	2017-01-11	2017-01-27	5.0	None	Remote	Low	Not required	None	None	Partial

Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.

2	CVE-2015-8994	264	+Priv	2017-03-02	2017-03-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.

3	CVE-2015-8876		DoS	2016-05-21	2016-05-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution via crafted serialized data.

4	CVE-2015-0232		DoS Exec Code	2015-01-27	2016-12-30	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.

5	CVE-2015-0231		Exec Code	2015-01-27	2016-12-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.

6	CVE-2014-9912	119	DoS Overflow	2017-01-04	2017-01-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.

7	CVE-2014-9427	119	Exec Code Overflow +Info	2015-01-02	2016-12-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.

8	CVE-2014-5459	59		2014-09-27	2016-10-25	3.6	None	Local	Low	Not required	None	Partial	Partial

The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.

9	CVE-2014-5120	20		2014-08-22	2016-10-25	6.4	None	Remote	Low	Not required	None	Partial	Partial

gd_ctx.c in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) imagegd, (2) imagegd2, (3) imagegif, (4) imagejpeg, (5) imagepng, (6) imagewbmp, or (7) imagewebp function.

10	CVE-2014-4721	200	+Info	2014-07-06	2017-01-06	2.6	None	Remote	High	Not required	Partial	None	None

The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.

11	CVE-2014-3670	119	DoS Exec Code Overflow Mem. Corr.	2014-10-29	2016-10-17	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.

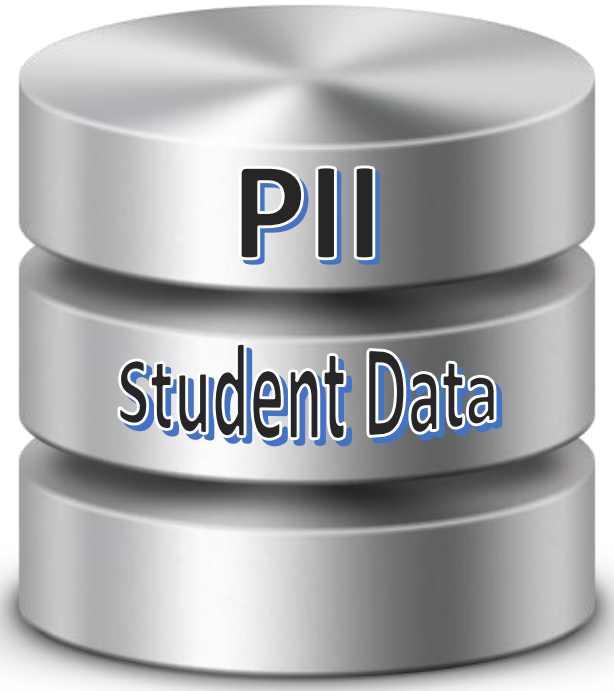
12	CVE-2014-3669	189	DoS Exec Code Overflow	2014-10-29	2017-01-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.

13	CVE-2014-3668	119	DoS Overflow	2014-10-29	2016-10-17	5.0	None	Remote	Low	Not required	None	None	Partial

Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.

Database Exposure



MongoDB Instances (No Authentication)

62

TOP COUNTRIES

United States	62

TOP CITIES

Chicago	6
West Lafayette	2
Seattle	2
Philadelphia	2
Los Angeles	2

Extortion as a result of misconfigured service

```
_id: ObjectID('597534461c3859926222067d')
email: "textme@secmail.pro"
btc_wallet: "151ExgNqvuqu4yXZEB9tzVpkr7CMHuZkup"
note: "We have your data. Your database is backed up to our servers. If you want to restore it, then send 0.15 BTC and te
     xt me to email, just send your IP-address."
```

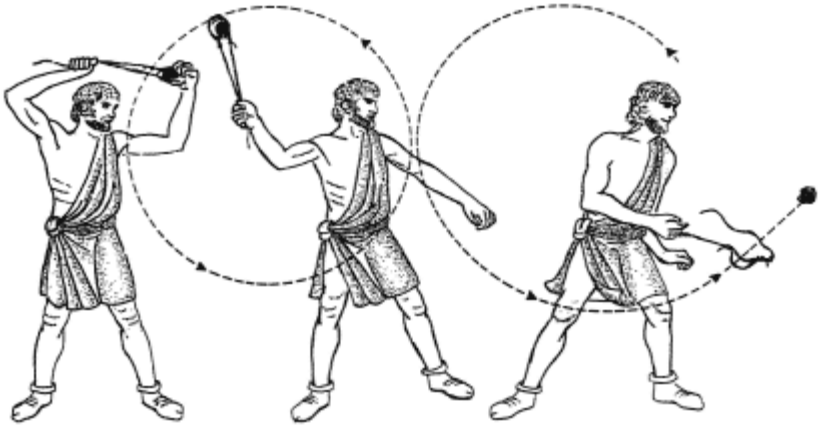
Is it hot in here??

Internet of Things (IoT) and Industrial Control System (ICS) attacks

- *University Baseball Stadium*
- *School thermostats*
- *Thousands of IP cameras*
- *Hundreds of access control stations (door controls, badge swipe, etc)*

The Reality is

Attackers only have to get lucky once…



Threats to Data

Internal

- Mistakes
- Intentional misconduct
- Curiosity

External

- Hackers
- Social engineering attacks
- Malware

Understanding the Threat

Key points to understand:

1. Data **will** get breached
2. You will **never** have enough resources to be "secure"
3. It is about **how** you prepare

Social Engineering

"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."

Social Engineering

- Phishing emails.
- Spear Phishing & Whaling.
- Telephone calls / SMS messages.
- Baiting.
- Watering hole attacks.
- Scareware.

Nearly every successful intrusion involves some form of Social Engineering!

Phishing Awareness - Example

Greetings to you my friend,

I know this will come to you as a surprise because you do not know me.
I am John Alison I work in Central Bank of Nigeria, packaging and courier department.

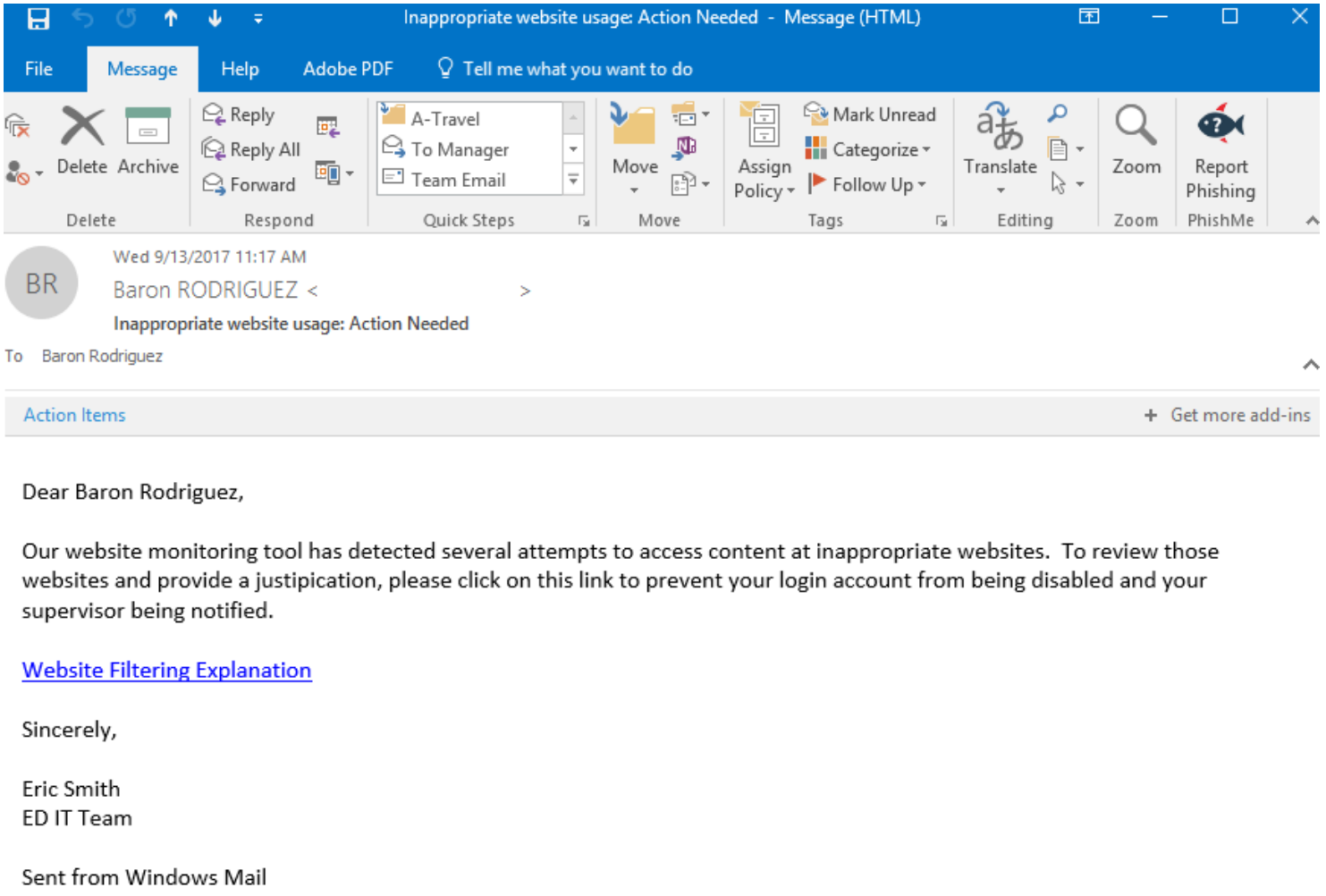
I got your contact among others from a search on the internet and I was inspired to seek your co-operation, I want you to help me clear this consignment that is already in theEurope which I shipped through our CBN accredited courier agent. The content of the package is $20,000,000.00 all in $100 bills, but the courier company does not know that the consignment contains money.

All I want you to do for me now is to give me your mailing address, your private phone and fax number, and I believe that at the end of the day you will have 50% and 50% will be for me. My identity must not be revealed to anybody.

If this arrangement is okay by you, you can call

Phone: +234 8028776685
Email:john_alison444@yahoo.com

Feeling Guilty?



Phishing Awareness

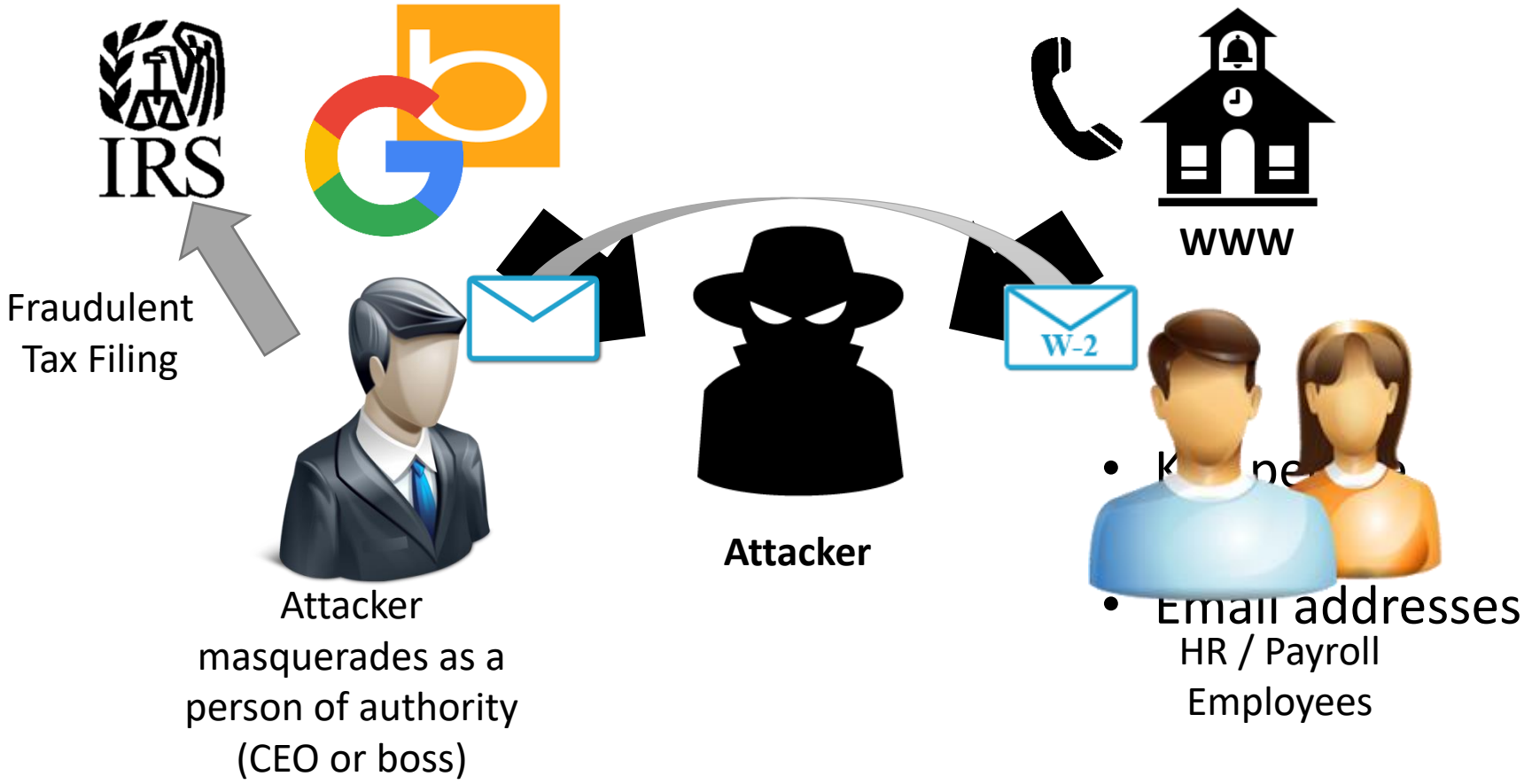
Most phishing e-mails are easy to notice. Here are some things a sophisticated hacker to do to gain access to your systems.

1. *Locate Staff Directory (yes, it's there).*
2. *Send Phishing E-mail to targeted employees, infecting the unwary user.*
3. *Locate and exfiltrate data, pwn everything.*
4. *Profit!*

2017 W-2 Phishing

- Now targeting Schools and Education Institutions.
- Spear-Phishing through email.
- Focus on HR / Payroll staff.
- Goal is to obtain employee data to file false returns.

2018 W-2 Phishing



Combating Social Engineering

- Train users on information security annually.
- Training should include phishing / safe browsing habits like:
  - Being wary of unsolicited email from untrusted sources.
  - Ensuring connections are secure.
  - Validating links before clicking.
- Make sure employees know who to contact in the event of an issue.
- Do not rely on technology alone.

What to do - Organizationally

- Make good, reasonable policy that is backed by leadership.
- Do a risk assessment, determine your risk threshold.
- Training coupled with security awareness updates.
- Develop an incident response plan.
  - Train staff on the plan
  - Test the plan
- Think like a hacker!

Security Tips for Users

Enterprise controls only extend to the network boundary. Users take their devices on the road, to the airport and the local coffee shop. Here are what users can do to protect themselves when away from the office:

- *Be aware of common threats affecting users.*
- *Take steps to reduce risk.*

What to do - Individually

- Use encryption. SSL/TLS, VPN, Full-disk, file level.
- Verify website are secure by visually checking.
- Treat all WiFi as untrusted WiFi.
- Check links in emails and documents before clicking through them.
- Never plug in a strange flash drive.
- Set a screen lock.
- Patch and update regularly, especially for third party applications.
- Use strong passwords.

Passwords: How good is this password?

- zQ4ab!ui

It would take a computer about

9 HOURS

to crack your password

How about this Password?

- I L0ve my M0m!

It would take a computer about

429 BILLION YEARS

to crack your password

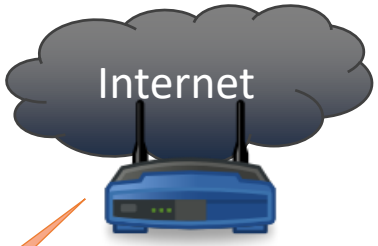
Security Tips for Users

Wi-Fi can be convenient, but using free Wi-Fi carries some risks:

- Fake access points can lure you into connecting to a hacker's system.
- Man-in-the-middle attacks can expose sensitive data in transit.

Security Tips for Users

- The user is connected to their local free wireless access point called “FreeWiFi”.



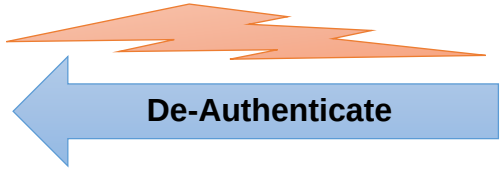
FreeWiFi

The Attacker is now the service provider for the User and is able to see and manipulate the User’s network traffic

The Attacker then creates his own access point with the same Service Set Identifier (SSID).

The Client’s computer then reconnects to what it thinks is the same “FreeWiFi” network.

Wireless User



The attacker sends a spoofed message pretending to be the access point instructing the User’s computer to disconnect .

Attacker

“Hey there, I am FreeWiFi. Connect to me!”

Security Tips for Users

- Avoid using untrusted networks to do sensitive things.
- If you must, use Virtual Private Network (VPN) technologies to secure your access.
- Don’t join wireless networks automatically or just turn off Wi-Fi unless you need it.
- Be wary of odd behavior on free Wi-Fi networks, like frequent disconnects, slow performance or certificate warnings.
- Employ strong WPA2 encryption for your own wireless networks with a long and complex passphrase.

Questions?

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

http://studentprivacy.ed.gov

(855) 249-3073