



Cybersecurity: You Make Your Own Luck

WISE Data Conference

Ross Lemke

Director

Privacy Technical Assistance Center (PTAC)

Disclaimer

This content was produced by the U.S. Department of Education's Student Privacy Policy Office (SPPO) through its Privacy Technical Assistance Center (PTAC) for the purposes of this presentation. This presentation is provided for informational purposes only. Nothing in this presentation constitutes official policy or guidance from the U.S. Department of Education.

Official policy and guidance can be found on our website at <https://studentprivacy.ed.gov/>.

What is most likely?

- A. Your school will fall victim to a brand new 0-day vulnerability causing a major data breach
- B. Your organization is targeted by a cyber criminal gang that over the course of a year hack into the district network
- C. Someone user give the bad guys their password inadvertently

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?



Things that Happened in 1974



FERPA

Family Educational
Rights & Privacy Act



FERPA & Data Security

While FERPA doesn't specify what security controls & technology, it does require you to protect PII from student records from disclosure and to:

- *Ensure that school officials obtain access to only those education records in which they have legitimate educational interests*
- *Identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses PII from education records*
- *Ensure to the greatest extent practicable that any entity or individual designated as its authorized representative uses, protects, and maintains / destroys data in accordance with FERPA requirements*

8

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



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

The Internet is Bad Neighborhood

Your data is only milliseconds away from every jerk on the planet

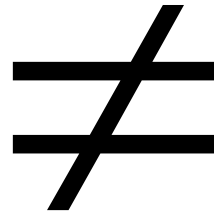
- *Malware / Ransomware*
- *Phishing & Social Engineering*
- *Hackers*
- *Denial of Service*
- *Those guys who comment bomb your social media status*



Understanding the Threat – K12



Cyber budget = \$15 Billion



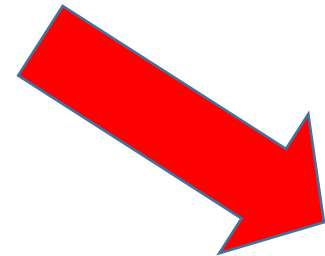
Cyber Budget = Gym Teacher

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
- Passwords
- Vendor / Cloud vulnerabilities
- People

Let's Just Start Here

| | |
|----------------------------|--------|
| Windows | 49,917 |
| Ubuntu | 11,516 |
| Windows (Build 10.0.19041) | 6,962 |
| Linux | 6,197 |
| Mac OS X | 4,547 |
| Debian | 1,694 |
| PAN-OS | 1,561 |
| Unix | 1,209 |
| Windows (Build 10.0.17763) | 1,080 |
| Windows (Build 10.0.14393) | 950 |
| Windows (Build 6.3.9600) | 916 |
| Playstation 4 | 448 |



Legacy Software Sticks Out to Hackers

Login

4.0.2

Username:

Password:

Login



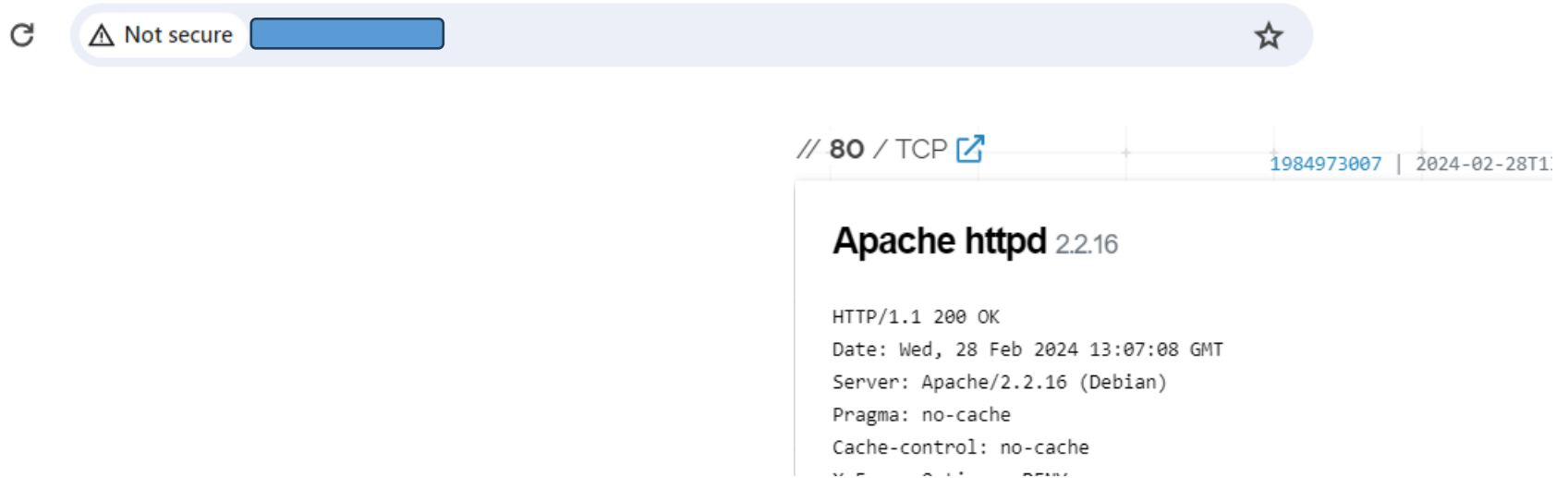
»|« RT 4.0.2 Copyright 1996-2011 Best Practical Solutions, LLC.

Distributed under version 2 of the GNU GPL.

To inquire about support, training, custom development or licensing, please contact sales@bestpractical.com.



Legacy Software Sticks Out to Hackers



CVE-2021-40438

 Known exploited

A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

Max CVSS

9.0

EPSS Score

97.37%

Published

2021-09-16

Updated

2022-10-05

CISA KEV

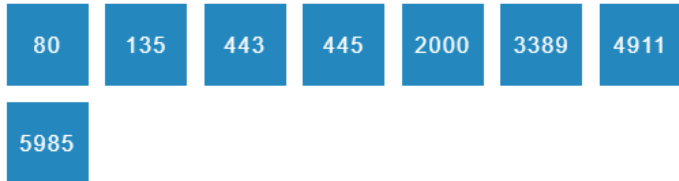
2021-12-01

Added



HVAC is the new Hotness

Open Ports



HVAC is the new Hotness

SMB Status:

Authentication: enabled

SMB Version: 1

Say
Cheese...
To RCE on
your
Cameras

Hikvision IP Camera:

Web Version: 4.0.51 build 171127

Plugin Version: 3.0.6.2701

Custom Version: DZ20171023_061

ActiveX Files:

AudioIntercom.dll: 1.4.0.3

LTSWebVideoActiveX.ocx: 3.0.6.2701

NetStream.dll: 1.0.5.41

npLTSWebVideoPlugin.dll: 3.0.6.2701

PlayCtrl.dll: 7.3.3.62

StreamTransClient.dll: 1.1.3.7

SystemTransform.dll: 2.5.2.5

IoT = Internet of (Terrible) Things



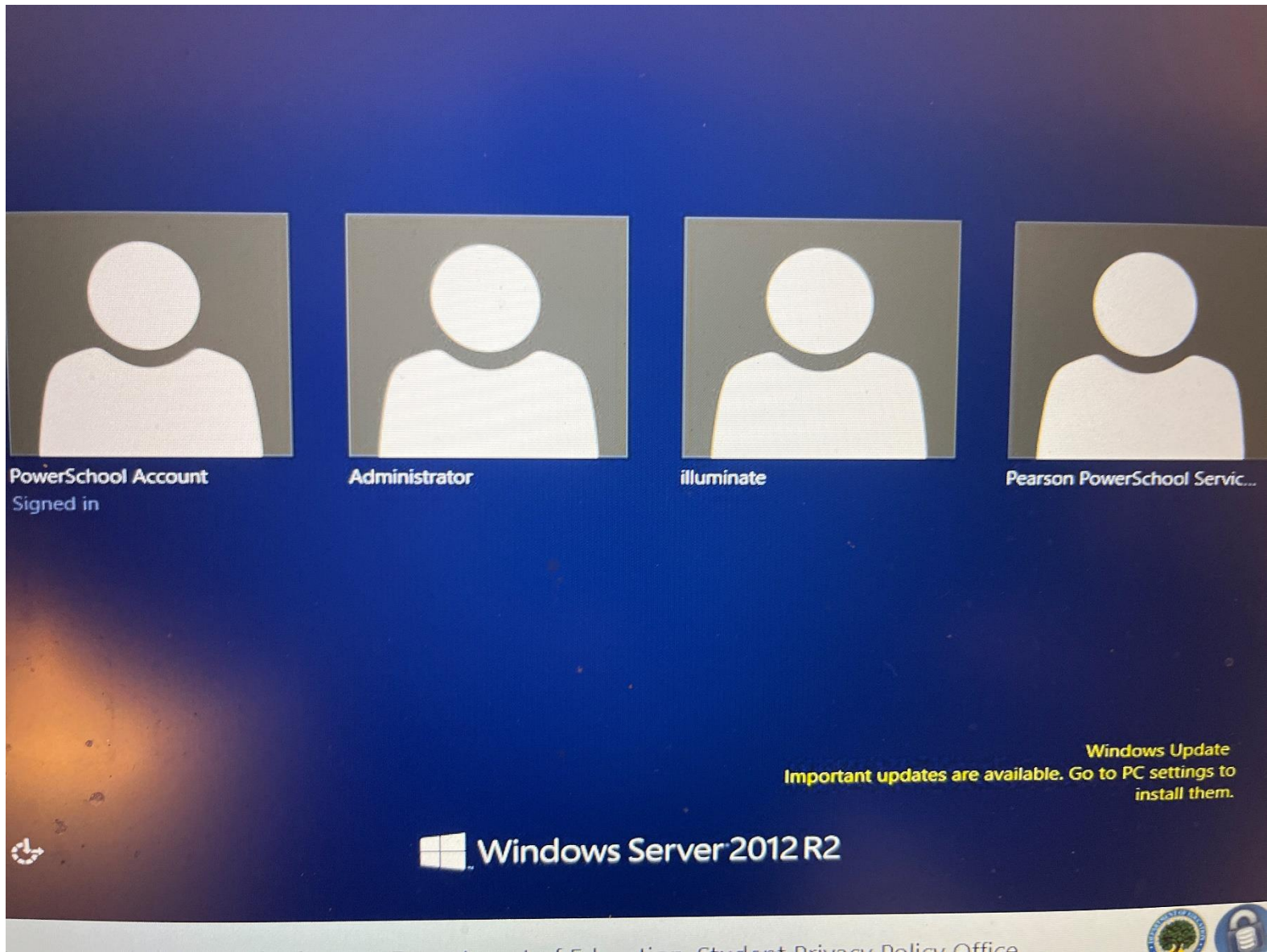
```
{ "confirmWizard": "Enable the wizard?", "configWizard": "Wizard", "wizardTitle":  
"The wizard helps you to configure the following settings:", "wizardContent1": "Edit  
the password of admin user.", "wizardContent2": "Configure WAN settings.",  
"wizardContent3": "Configure WIFI settings.", "wizardContent4": "Initialize HDD.",  
"wizardContent5": "Add IP cameras.", "wizardContent6": "Configure record  
schedule.", "exitWizard": "Exit", "oldPassword": "Admin Password",  
"newPassword": "New Admin Password", "oldPasswordInvalid": "Incorrect Admin  
Password.", "channelList": "Camera List", "allDayPlan": "All-day Recording" }
```

```
153     cmd = cmd.gsub(%r{tmp/[0-9a-zA-Z]+}, @fname)  
154     cmd = cmd.gsub(/ >/, '>')  
155     cmd = cmd.gsub(/> /, '>')  
156  
157     payload = "<xml><language>${#{cmd}}</language></xml>"  
158     res = send_request_cgi({  
159         'method' => 'PUT',  
160         'uri' => normalize_uri(target_uri.path, '/SDK/webLanguage'),  
161         'data' => payload  
162     })
```



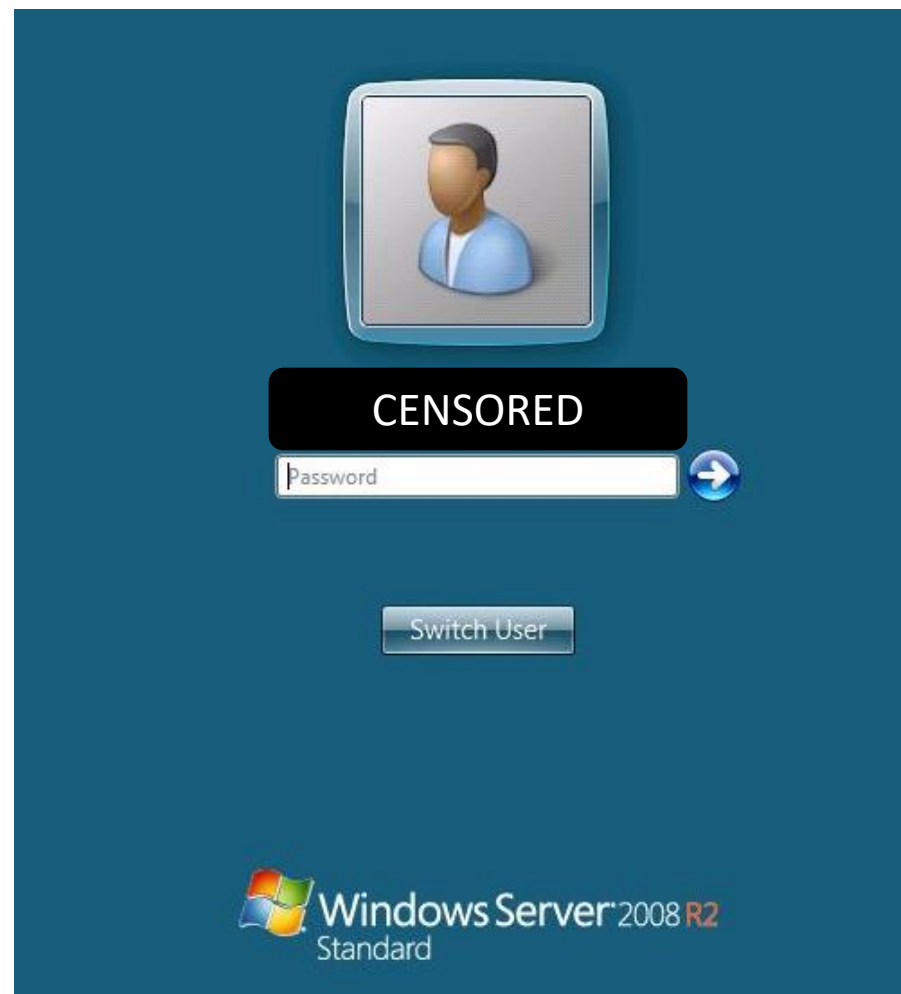






End of Life = Vulnerable

- Windows 2008 r2
- End of life was January of 2020
- Vulnerable to BlueKeep (CVE-2019-0708)
- *Also, potentially three other vulnerabilities impacting IIS 7.5*





Administrator



Local Administrator



staff

Cancel

 Windows Server 2008 R2
Standard



DNSAdmin

Windows Update
Important updates are available. Go to PC settings to install them.



 Windows Server 2012 R2



The Reigning Champ!!

21

tcp

ftp

IBM OS/2 ftpd

220 [REDACTED] IBM TCP/IP for OS/2 - FTP Server ver 17:11:22 on Feb 4 1999 ready.

230 Guest login ok, access restrictions apply.

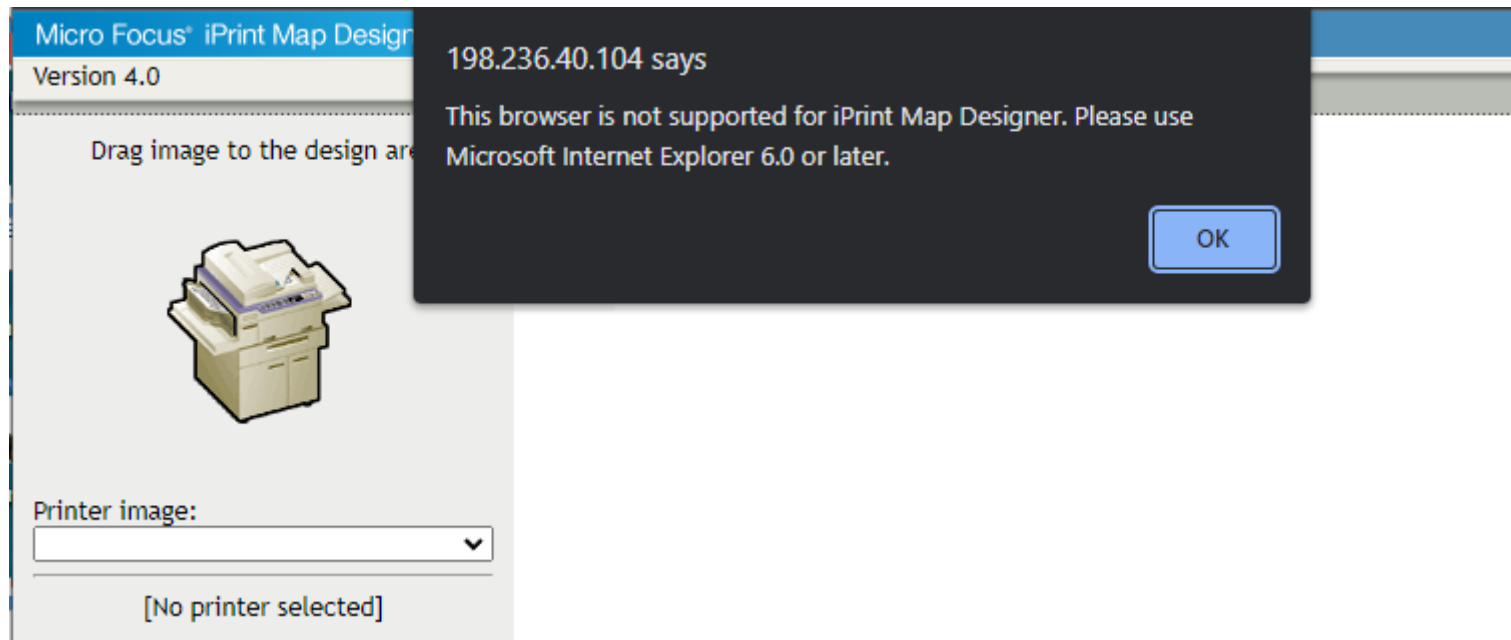
214- The following commands are recognized (* =>'s unimplemented).

| | | | | | | | |
|-------|------|-------|-------|------|------|------|------|
| USER | PORT | STOR | MSAM* | RNTO | NLST | MKD | CDUP |
| PASS | PASV | APPE | MRSQ* | ABOR | SITE | XMKD | XCUP |
| ACCT* | TYPE | MLFL* | MRCP* | DELE | SYST | RMD | STOU |
| SMNT* | STRU | MAIL* | ALLO | CWD | STAT | XRMD | SIZE |
| REIN* | MODE | MSND* | REST* | XCWD | HELP | PWD | MDTM |
| QUIT | RETR | MSOM* | RNFR | LIST | NOOP | XPWD | |

214 Remote help successful.

502 Unknown command.

You know it's up to date when



IoT / ICS Exposure

- This likely controls HVAC or other facilities operations
- Why do you need this access from the internet?
- This product has had significant vulnerabilities in the past regarding unrestricted file uploads (CVE [2017-9650](#)) and path traversal and arbitrary file write issues ([CVE 2017-9640](#))
- Do serial numbers need to be disclosed to anyone who stumbles on this page? Could they be used to phish a password reset or other services from the support?






Change Your Passwords...

Because these exist:

IP camera default password list

| Camera Manufacturer | Username | Password |
|---------------------|---------------|----------|
| 3xLogic | admin | 12345 |
| ACTi | Admin | 123456 |
| ACTi | admin | 123456 |
| Amcrest | admin | admin |
| American Dynamics | admin | admin |
| American Dynamics | admin | 9999 |
| Arecont Vision | admin | <blank> |
| AvertX | admin | 1234 |
| Avigilon | admin | admin |
| Avigilon | administrator | <blank> |
| Axis | root | pass |
| Axis | root | <blank> |
| Basler | admin | admin |
| Bosch | <blank> | <blank> |
| Bosch | service | service |

 You are not allowed to print or save this page!!

Access Controllers

- HID VertX door controller
- Up to 32 door controllers on a single network interface
- They are popular in schools and SEAs

Access Controllers

- Vulnerable service “discoveryd”
- Remote Command Execution
- Lock and Unlock doors
- Download access control cards
- Execute any command as “root” user


Information Just Wants to be Free

RICOH MP C306Z Web Image Monitor

← Home

Shared Folder







Back

 Delete


View : All Search : File Name : Search

1/1 Page(s) : GO Display Items : 10

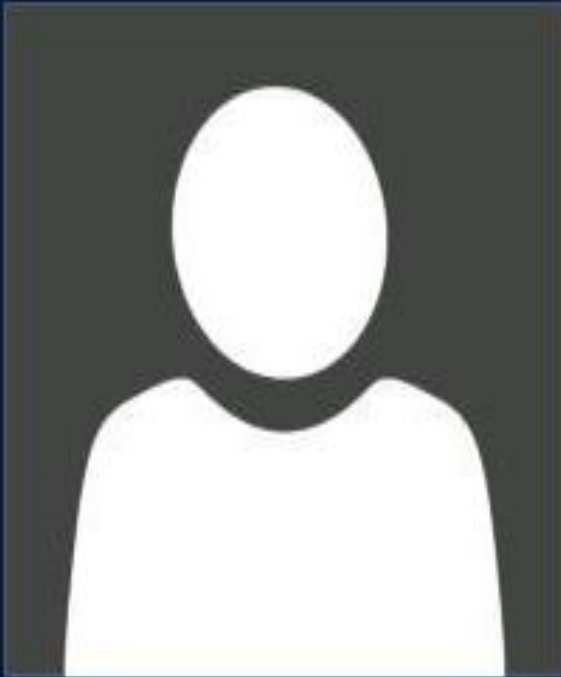
Total Files : 3 Selected Files : 0 Uncheck All

| | | |
|--|---|--|
| <input type="checkbox"/> NEW IG INT Reference Download   | <input type="checkbox"/> SCAN0001 Download   | <input type="checkbox"/> DRED/DSS reference Download   |
|--|---|--|



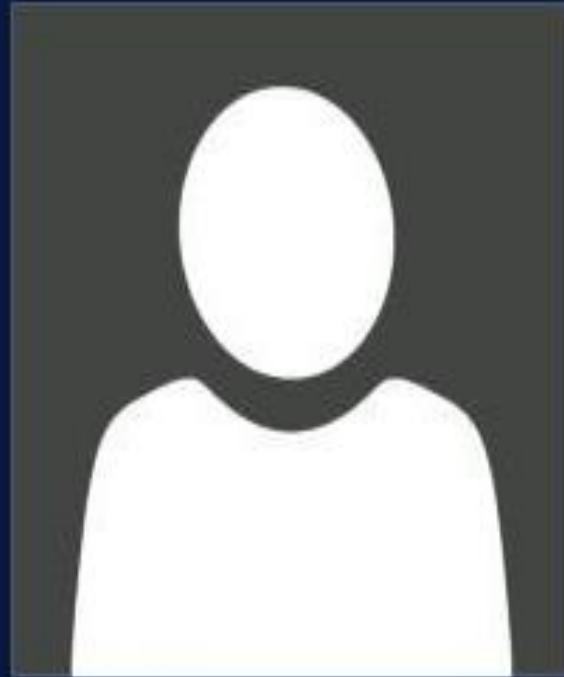


People – Your
Employees are the
Weakest Link



Paul CENSORED

CENSORED prcadmin



Other user

How Attackers Exploit this Info

- Start high level and look at his papers, slides and emails to spot weaknesses in the enterprise
- Target with spear phishing / whaling attacks to phone, email, SMS
- Impersonation attacks against staff at the school
- Leverage friends & colleagues names to elicit action or shift focus to them
- Failing that, there's always blackmail, intimidation, coercion and threats

How a Organizations are Vulnerable

**Most phishing e-mails are easy to notice.
Here are some things an attacker might 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
4. Profit!

Isn't this
someone
else's
problem?

- **Most breaches start with social engineering**
- **Attackers target YOU, not the technology first**
- **Most successful large breaches use stolen credentials!!!!!!!**

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***
- ***Take concrete 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.
- Use strong passwords.
- Multi-factor authentication is your friend
- 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.

Data Security is a Shared Responsibility

IT

- Vulnerability Mgmt
- Account Mgmt
- Boundary Control
- Performance Metrics

Shared

- Privacy & Security Training
- Incident Response
- Risk Management
- Data Accountability

Tailor Data Security to Your Business

Do not forget that the purpose of the systems is to enable the business of educating children!

Security



Utility

Perform Annual Risk Assessments

“The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.”

-National Institute of Standards and Technology (NIST)

What is a Risk Assessment?

Formal organizational process involving leadership, IT, and organizational stakeholders

Four stages:

- **Identification** – *finding, documenting, and categorizing risks*
- **Analysis** – *ascertaining the nature of the risks and determining their potential impact and effects*
- **Evaluation** – *applying organizational risk tolerance and existing controls to the risk to determine significance*
- **Control** – identifying and applying mitigating controls to reduce the risk based on analysis

Data Security

Bare Bones Must Haves:

For a Strong Data Security Foundation

- Privacy & IT security Training annually
- Agile Vulnerability Management
- Formalized Risk Management Processes
- Incident Response Plan & Team
- Strong Account Management
- Adopt Common Data & System Standards
- Enforcement of Standards

The Reality is

Attackers only have to get lucky once...

So, Think Like a Hacker!

- *Get outside the boundary*
- *Survey what is exposed*
- *Stop thinking about what you need to defend*
- *Start thinking about how YOU would attack?*



Put on the Black Hat!

You are the most qualified attackers of your own systems!

Attackers would love to know what you know about your systems

Use your knowledge of your systems to your advantage to identify risks

Find the “Low Hanging Fruit” before the bad guys do

Enjoy better sleep, savings on insurance rates, less painful audits, and better privacy and security

From the Attacker's Perspective

- ***Lowest Hanging Fruit***
 - easy wins
 - legacy software
 - bad permissions
 - misconfigurations
- ***Social Engineering***
 - Phishing
 - Baiting
 - Pre-texting
 - Watering hole attacks



Search Engines for Fun & Profit



a hacker's best friend:

GHDB – Google Hacking Database

A website that contains a library of pre-configured Google searches (Google Dorks)

- <https://www.exploit-db.com/google-hacking-database>
- Allows you to quickly build highly targeted searches to find “interesting” information
- Categories like “Files containing Passwords” and “Sensitive Directories” and “Vulnerable Servers”

Data Breach Reporting

Consider calling PTAC!

We can help by providing:

- *Technical / Compliance Assistance*
- *Access to resources*
- *Training*
- *Moral support and virtual hugs.....*

We have all been there, and we really want to help!

Questions?



CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center



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



privacyTA@ed.gov



<https://studentprivacy.ed.gov>



(855) 249-3073

Thank you!



Thank you!

**Please scan the QR code to provide us with
your feedback!**