



How NOT To Be the Slowest Zebra:

The State of Cybersecurity in Schools
WISEdata

March 2023



Ross Lemke

Privacy Technical Assistance Center (PTAC)





What is

- A. Your district's new 0-day vulnerability
- B. Your district's gang that the district
- C. Someone's bad guys that



and new 0-
data breach
criminal
hack into
the bad

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



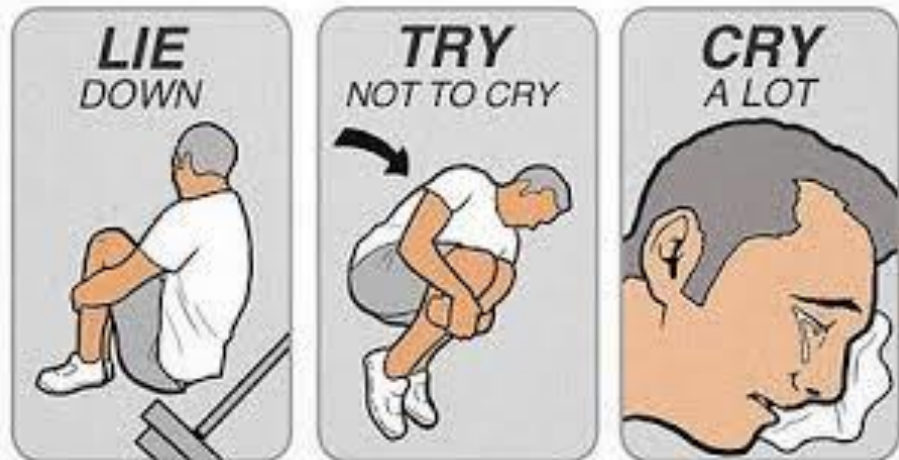
FERPA & Data Security

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*

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

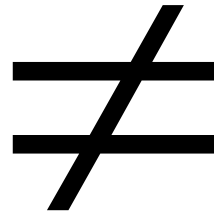


Understanding the Threat

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

Understanding the Threat – K12



Cyber budget = \$15 Billion

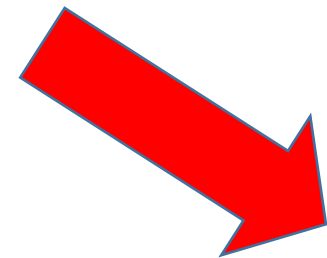
Cyber Budget = Gym Teacher

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



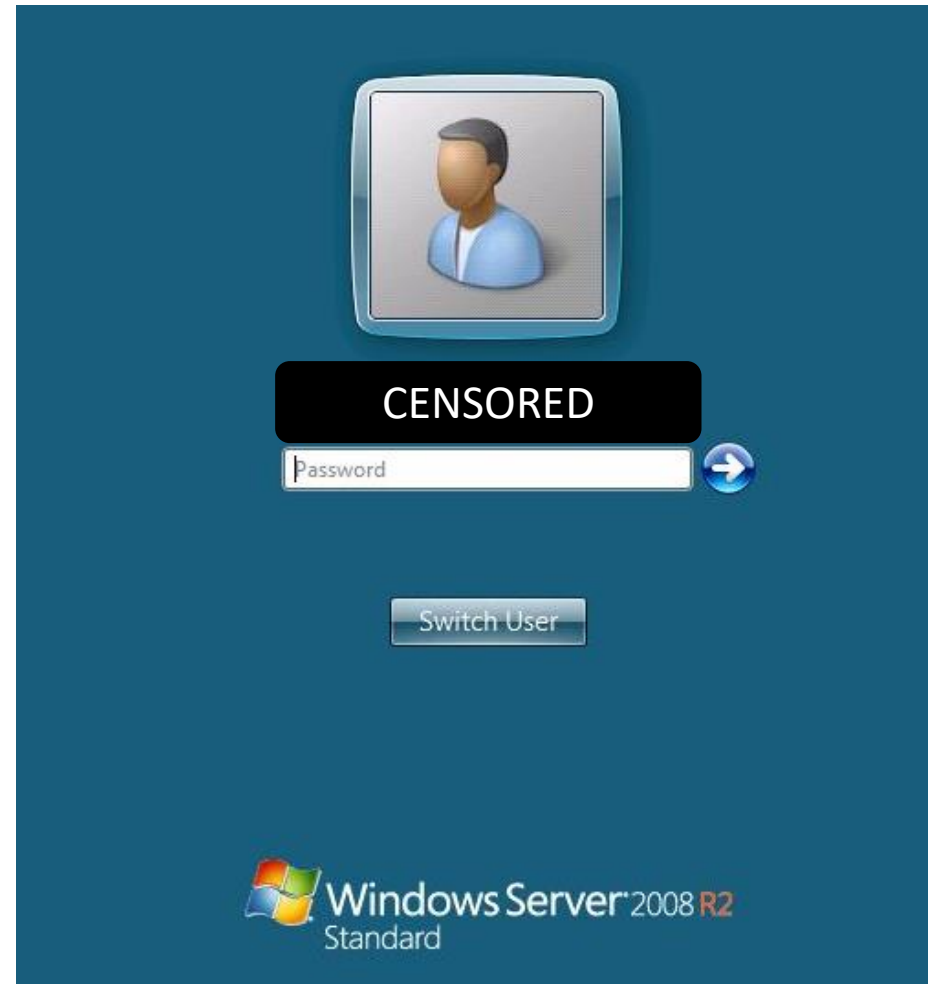






End of Life = Vulnerable

- 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*





DNSAdmin

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



 Windows Server 2012 R2

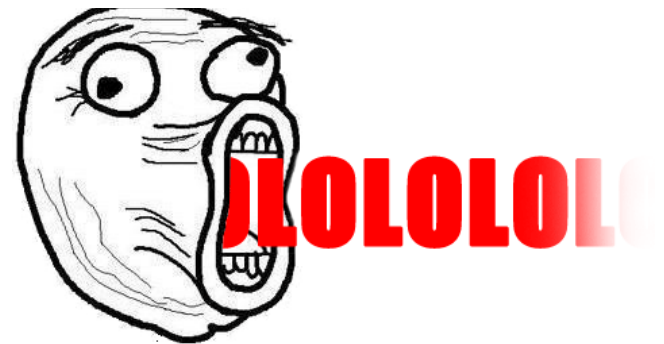


The Reigning Champ!!

21
tcp
ftp

IBM OS/2 ftpd

```
220 m3 [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.
```



Speaking of File Transfer

This is a public internet facing school web application that enables anyone on the internet to spoof any sender to send a file to any recipient with no apparent safety checks from a school domain.

Your Name

Your Email

Recipient Email(s)

Put each address on its own line.

Message to Recipient
(optional)

Expiry day(s) Password Show

File(s)
 No file chosen
Maximum file size is 1 gigabyte.

Speaking of File Transfer

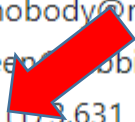
Maximum file size is 1 gigabyte.

In case you were wondering...

Here is an email I sent myself containing a cat meme...

I mean what could go wrong?

From: John (nobody@nowhere.net)
To: redqueen@rabbit-hole.org
File: [cat.jpg](#) (173,631 bytes)
Date: 10/14/2022 9:09pm
Expires: 10/21/2022 9:09pm



File Available



CENSORED

To redqueen@rabbit-hole.org

This might be a phishing message and is potentially unsafe. Links and other functi

Hello,

You have received a file from John.

=====
Sender comments:

Test
=====

Pick up your file:

[https://CENSORED/get/CDdcy3hDmCzN4Ak5hbU7D1GMfGBFuaC9](#)


Your file will expire in 7 days.

CENSORED

PHP... aging like fine wine

- PHP 5.6.40 has been unsupported for going on 4 years now
- That means no more security patches have been installed since December of 2018
- Do you think hackers stop finding exploits when the software is dead?

```
// 443 / TCP ↗  
  
Apache httpd 2.4.6  
  
HTTP/1.1 200 OK  
Date: Sun, 02 Oct 2022 16:16 GMT  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40  
X-Powered-By: PHP/5.6.40
```

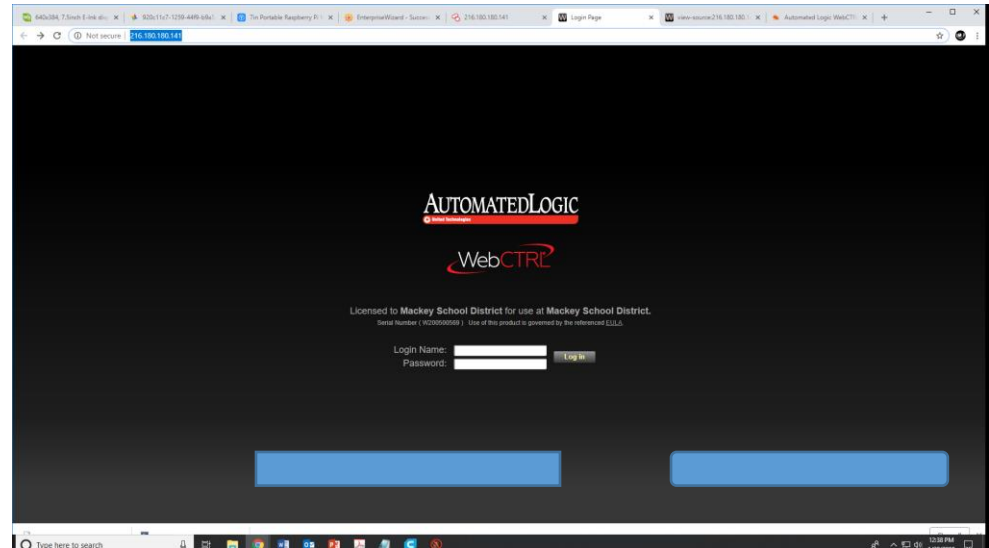


You know it's up to date when



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?



IoT / ICS Exposure

*Well at least
you know right
where you are*

**Version missing!
Version conflict!**

Instrument ID:	6760	Uptime:	132 days 22:37 h	Logging:	Off	GPS		SBAS	
Receiver type:	GRX1200 GG Pro	Memory:	24% (7.41 MB)	RTK:	Off	GLONASS		Oscillator	
IP address:	192.168.0.3	Power:	79%	Ring buffer:	Off	GALILEO		21-10-03 2023-02-03	

[Home](#) | [Status](#) | [Configuration](#) | [Help](#) | [Support](#)

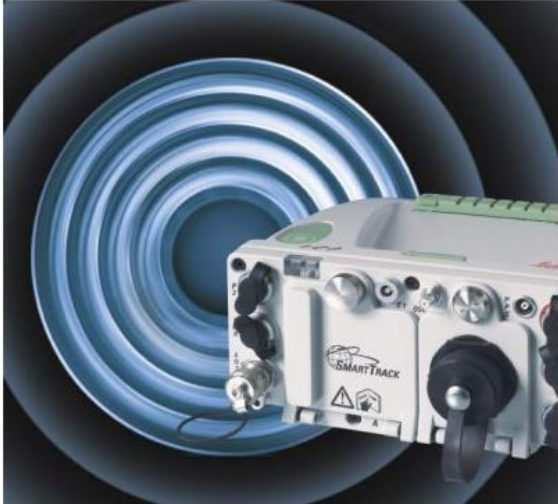
GRX1200 GG Pro

Status


- ↓ System Information
- ↓ Power & Memory
- ↓ Position
- ↓ Satellites
- ↓ Logging
- ↓ Antenna
- ↓ Message Log
- ↓ Interfaces
- ↓ Port summary
- ↓ CF Card (via FTP)

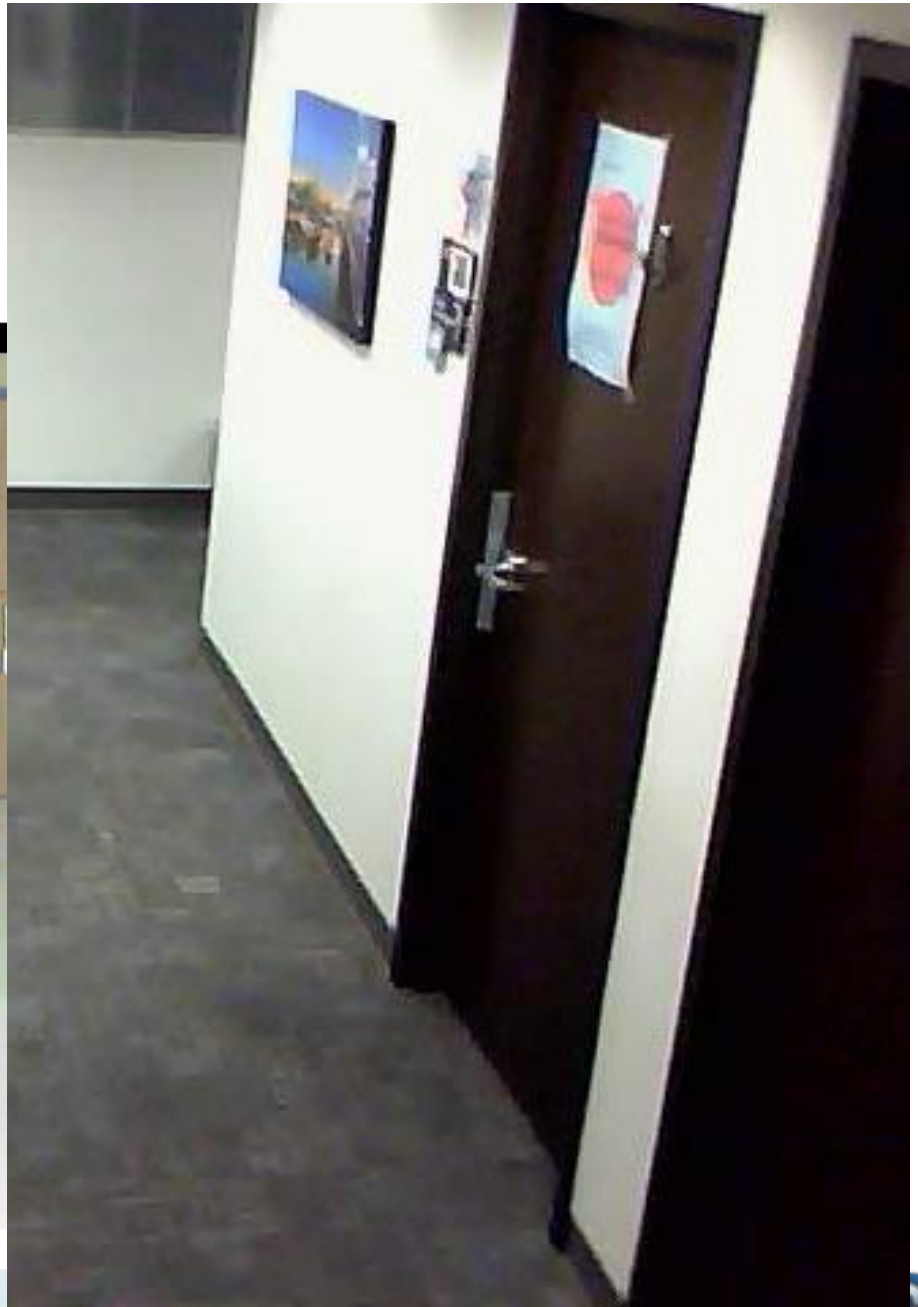
GRX1200 GG Pro - Web Interface

Welcome to the web interface for the GRX1200 GG Pro



© 2004-2005 Leica Geosystems





Change Your Passwords...

Because these exist:

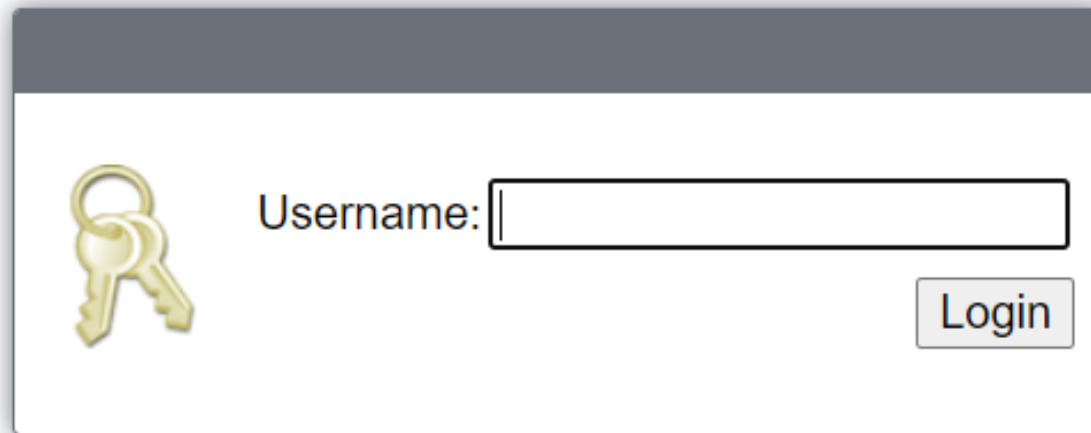
IP camera default password list

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
<blank>save this page!!

No More Patches?



A screenshot of a login interface. On the left is a gold key icon. To its right is the text 'Username:' followed by a rectangular input field. Further right is a button labeled 'Login'.

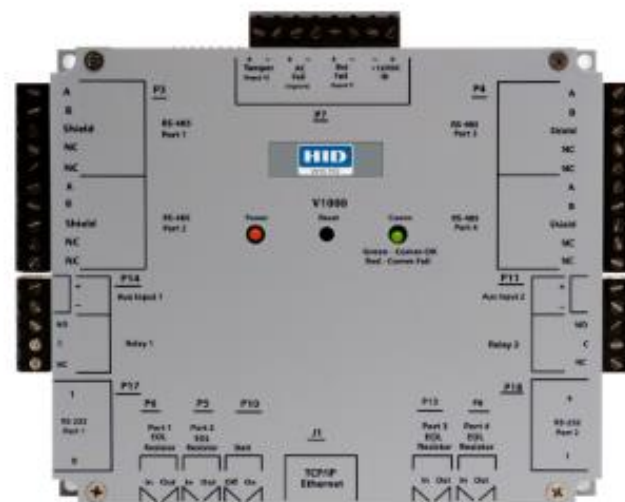
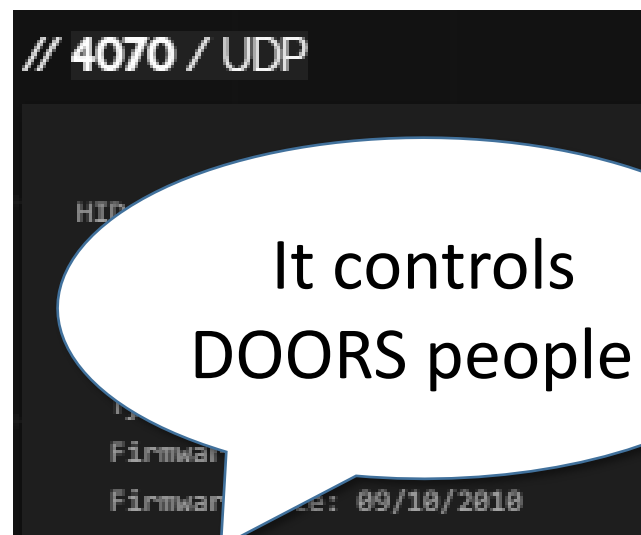
Use of this software is subject to the [End User License Agreement](#) and other [Third Party License](#)

Your Software Maintenance Agreement has expired.

To connect using Java Web Start [click here](#)
To connect using Niagara Web Launcher [click here](#)

Access Controllers

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



Access Controllers

Hackers Can Unlock Any HID Door Controller with One UDP Packet

Hacking like in the movies! Sometimes it's that easy


- 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

 Delete

View : Search : :

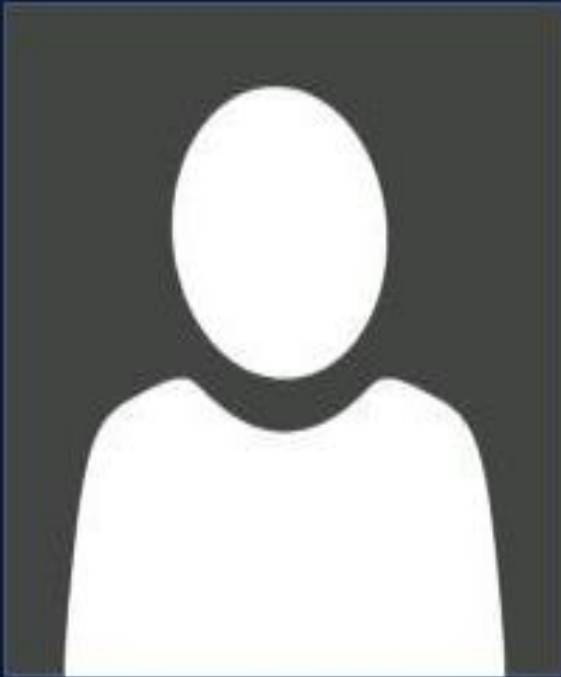
Page(s) : Display Items :

Total Files : 3 Selected Files : 0

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







Paul CENSORED

CENSORED prcadmin



Other user

Paul



[VIEW FULL REPORT](#) →



Landline number



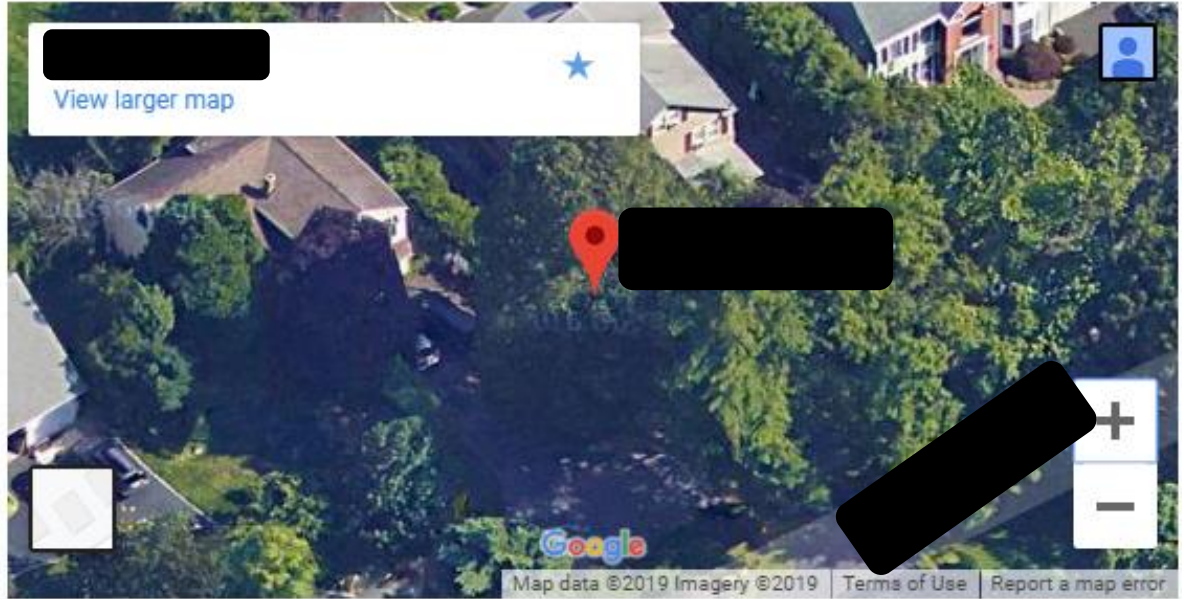
Mobile phone



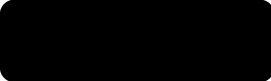
Email



Relatives



See more results for Paul



See more results for





CENSORED



textfiles.com_

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 Schools 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

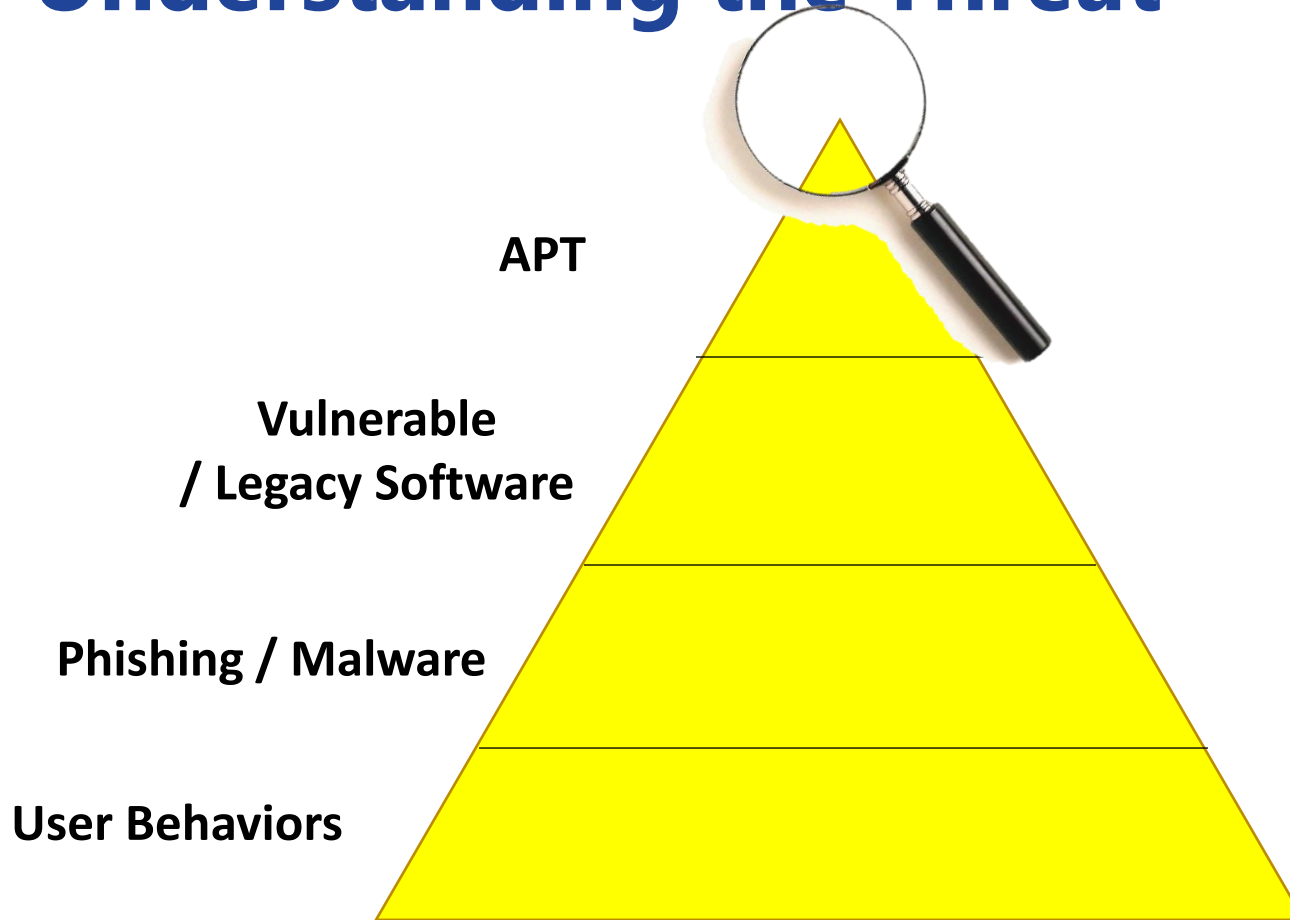
- Use encryption. SSL/TLS, VPN, Full-disk, file level.
- Verify website are secure by visually checking.
- Treat all WiFi as untrusted WiFi.
- Use strong passwords.
- Multi-factor authentication is your friend
- Check links in emails and documents before clicking through them.
- Never plug in a strange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



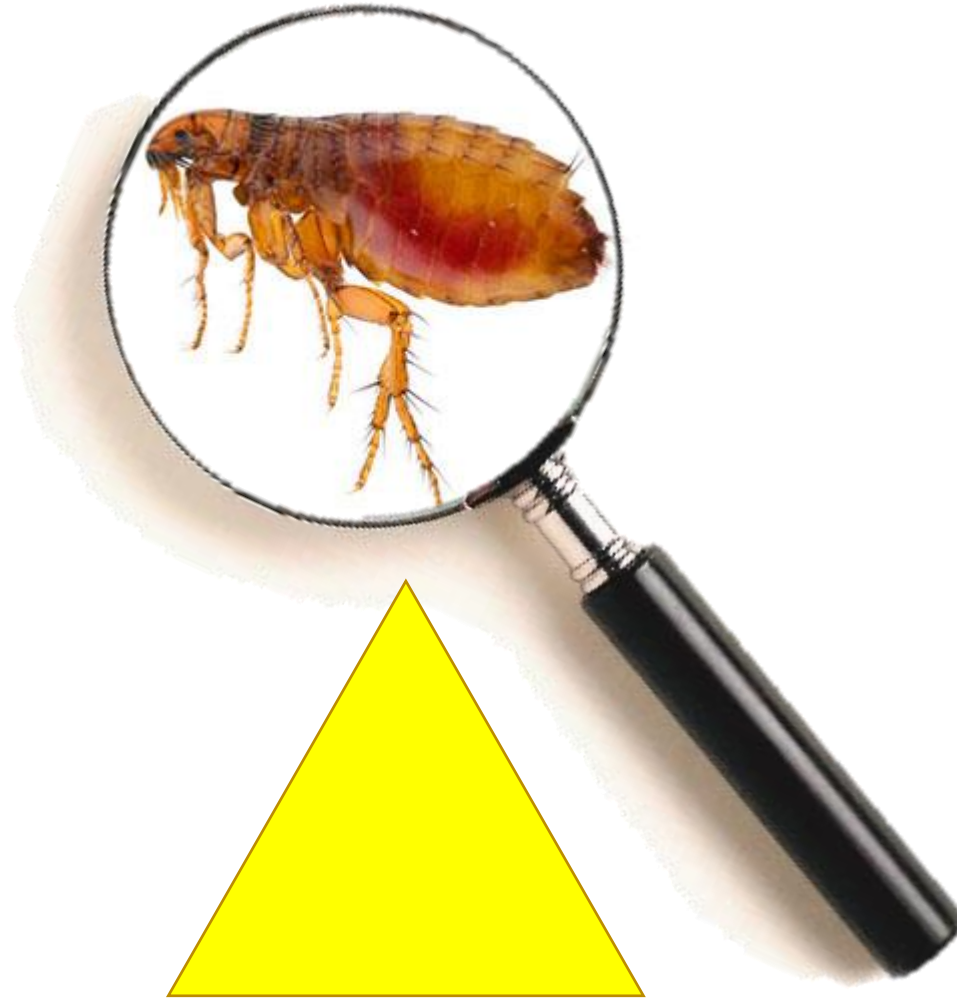
Understanding the Threat



Understanding the Threat



Understanding the Threat



Understanding the Threat



Understanding the Threat

A magnifying glass with a black handle and frame is positioned over the text '0-Day'. The lens of the magnifying glass is centered on the text, making it appear larger and more prominent. The background behind the magnifying glass is a blurred, warm-toned image, possibly of a person's face or a document.

0-Day

What to do - Organizationally

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
- Leadership Support

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

