Payroll Security

Why is everyone trying to hack me!?

What do modern thieves look like?
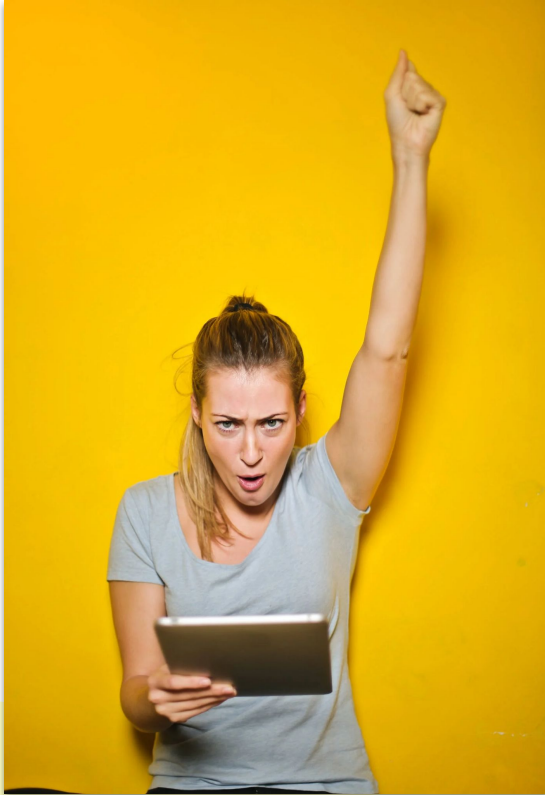
They almost always look like friends.

For years, attackers tried to

- Backdoor into your server
- Get access to your network
- Implant malware on your computer
- Or in some other way, get access to a system.

K12
MONTANA

The GOOD news is that

we stopped them!

The BAD news is that

we stopped them.

K12
MONTANA

What does this mean?

Bad guys are having a harder and harder time attacking our systems.

Google and Microsoft have helped.

Cloud technologies have helped.

Better password management has helped.

so…

Attackers now target YOU

- Attackers look for vulnerable parts of systems
- Technology used to be much more vulnerable
- People are inherently trusting
- Attackers are targeting people, instead of the technology itself.

K12
MONTANA

Still common…

Phishing - less effective than before

- General phishing attacks are still prevalent
- You likely receive several "spam" and suspicious phishing emails every week
- Your email client *probably* filters most (if not all) of these

K12 MONTANA

More common…

Spear Phishing - getting BIG

- Spear phishing is targeted
- Spear phishing is researched
- Spear phishing is personal
- Spear phishing preys on humanity

K12
MONTANA

And finally, Moby Dick

YOU are the big fish

Whaling (or Whale Phishing)

Spear phishing with focused intent

Targets the $$

How are the bad guys so effective?

Schools are transparent!

07 Cascade County

County Supt: Diane Heikkila   Phone:454-6855   E-mail: dheikkila@cascadecountymt.gov

Sun River Valley Pub Schls (SS:1067)
Box 380
Simms, MT 59477

	Phone/Extension	Fax
District Supt: Dave Marzolf	**264-5110 775**	**264-5189**
E-mail: dmarzolf@srvs.k12.mt.us		
District Clerk: Belinda Klick	**264-5110 122**	**264-5189**
E-mail: bklick@srvs.k12.mt.us		
Board Chairperson: Kennard Steinke	**264-5429**	**264-5189**
E-mail: amerifence@3rivers.net		

Simms H S (LE: 0118)   123 Walker Street
District No. F   Simms, MT 59477

		Phone/Ext	FAX	Grades Served
Simms High School (SC: 0174)		264-5110	264-5189	9-12
Principal LUKE MCKINLEY	123 Walker Street			
E-mail: lmckinley@srvs.k12.mt.us				

Sun River Valley Elem (LE: 1225)   123 Walker Street
District No. 55   Simms, MT 59477

		Phone/Ext	FAX	Grades Served
Cascade Colony School (SC: 1657)		264-5104	264-5265	PK-8
Principal HOLLY KINCAID	508 Birdtail Road			
E-mail: hkincaid@srvs.k12.mt.us				
Fort Shaw Elem School (SC: 0173)		264-5110	264-5146	PK-5
Principal HOLLY KINCAID	School Loop Road			
E-mail: hkincaid@srvs.k12.mt.us				
Sun River Middle School (SC: 1538)		264-5110	264-5189	6-8
Principal LUKE MCKINLEY	123 Walker Street			
E-mail: lmckinley@srvs.k12.mt.us				

07 Cascade County

County Supt: Diane Heikkila Phone:454-6855 E-mail: dheikkila@cascadecountymt.gov

Sun River Valley Pub Schls (SS:1067)
Box 380
Simms, MT 59477

	Phone/Extension	Fax
District Supt: **Dave Marzolf**	**264-5110 775**	**264-5189**
E-mail: dmarzolf@srvs.k12.mt.us		
District Clerk: **Belinda Klick**	**264-5110 122**	**264-5189**
E-mail: bklick@srvs.k12.mt.us		
Board Chairperson: **Kennard Steinke**	**264-5429**	**264-5189**
E-mail: amerifence@3rivers.net		

Simms H S (LE: 0118)
District No. F

123 Walker Street
Simms, MT 59477

		Phone/Ext	FAX	Grades Served
Simms High School (SC: 0174)		264-5110	264-5189	9-12
Principal LUKE MCKINLEY	123 Walker Street			
E-mail: lmckinley@srvs.k12.mt.us				

Sun River Valley Elem (LE: 1225)
District No. 55

123 Walker Street
Simms, MT 59477

		Phone/Ext	FAX	Grades Served
Cascade Colony School (SC: 1657)		264-5104	264-5265	PK-8
Principal HOLLY KINCAID	508 Birdtail Road			
E-mail: hkincaid@srvs.k12.mt.us				
Fort Shaw Elem School (SC: 0173)		264-5110	264-5146	PK-5
Principal HOLLY KINCAID	School Loop Road			
E-mail: hkincaid@srvs.k12.mt.us				
Sun River Middle School (SC: 1538)		264-5110	264-5189	6-8
Principal LUKE MCKINLEY	123 Walker Street			
E-mail: lmckinley@srvs.k12.mt.us				

K12
MONTANA

Sun River Valley
School District *55F*

About   School Board   Parents & Community   Contact   Educational Support   Clubs & Activities

About Us

Administration:
Superintendent (6-12): Dave Marzolf
Principal (6-12): Luke McKinley
Business Manager (6-12): Belinda Klick
Principal (K-5): Shianne Currey

K12
MONTANA

Sun River Valley School District *55F*

About   School Board   Parents & Community   Contact   Educational Support   Clubs & Activities

Staff

Search: [by name or position]

ADMINISTRATION

Mr. David Marzolf
Superintendent/Transportation Director

Mr. Luke McKinley
6-12 Principal/AD

Ms. Holly Kincaid
FSE Principal

K12 MONTANA

STAFF

Mrs. Becky Hart
IT

Mrs. Belinda Klick
Clerk/Business Manger

Mrs. Teri Nelson
Secretary

Mrs. Jennifer Rohrer
Business Teacher
Business Education

Privilege Escalation

Districts provide all of the information required for a type of attack we call Escalation Attacks - these are becoming more prevalent!

K12 MONTANA

Recent attacks

Escalation attacks are now common

Payroll attacks on the rise

Direct deposit schemes newest menace

Attacks are getting AWESOME

- The "From" email can be spoofed and look trusted
- Attacker's language and spelling are getting nearly perfect
- Sometimes the attack really DOES come from within!

K12 MONTANA

Anybody see this one?

And you probably saw this one…

Hello (yourname),

I have recently changed banks, can you update my payroll direct deposit information? Previous account on record will be inactive before my next payment day.

Regards,

(a real teacher)

Understand the blackmarket…

Throw seeds

(look for a target)

Cultivate

(nurture a target)

Harvest

(reap the final payout)

K12 MONTANA

From the Butte attack…

*"The email actually came from a cyber thief using **detailed information** illegally obtained from an **unknown source**, Jonart said. When school officials learned of the theft, the FBI, along with Homeland Security were notified."*

*"Jonart said it's still **not clear how the thief accessed the information** used to pull off the fraud, as a forensic investigator found the school district's accounts weren't subject to unauthorized access that would've led to the fraudulent wire transfer."*

- *© Montana Standard, Feb 19, 2023 - Kasey Faur*
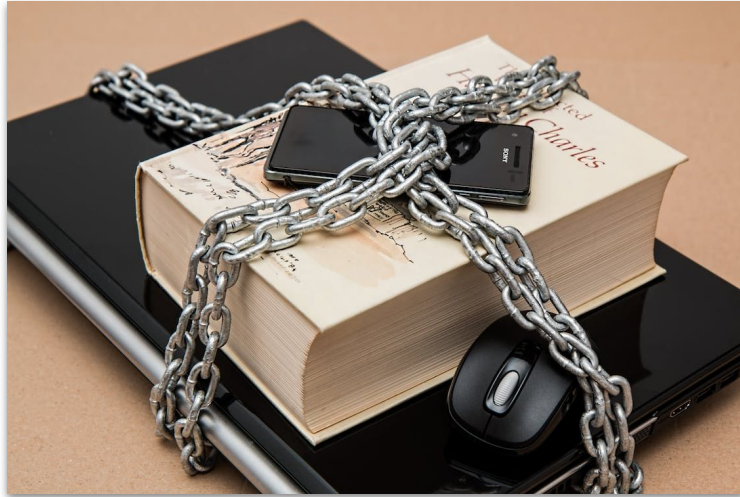
HOW do I defend my district?

TAKE CONTROL*s*

- Don't assume (remember what it makes!)
- Adopt procedures that protect everyone
- Get real signatures on internal $$ changes
- Verify, Verify, Verify! YOU call THEM
- Don't be concerned with looking foolish!

K12
MONTANA

Can technology help keep me safe?

…kinda…
But remember,
they attack *you* because
tech is already so good!

Changes to TECH / PROCEDURE

- Have your techs enable 2fa (at least for administration)
- Adjust policies to require signed paperwork for all employee banking
- Require POs for all suspicious/new vendors
- Be CAREFUL with direct deposits

K12
MONTANA

Pause & Think Online

Use your:

Head
Heart
Arms
Gut
Legs

YOU are the best defense!

Questions? Want a hand?

Jeff Patterson - jeffp@k12mt.com

K12 Montana - k12mt.com

We work across the state helping schools with a variety of projects and opportunities!