

Why amp up your Data Security?

492 Districts

have experienced a **cyberattack** since 2016.¹

THREATS



RANSOMWARE

"We'll destroy your data unless you pay us"

170:

COUNTY, CITY OR STATE GOVERNMENT SYSTEMS ATTACKED SINCE 2013.²



MALWARE

"We'll steal your information & break your stuff"

1,000:

COMPUTERS REBUILT BY OHIO DISTRICT'S IT STAFF AFTER A MALWARE ATTACK.³

KEYLOGGING

We'll use a sneaky device or software to steal all the info typed into your machine.



\$50:

PRICE OF A USB KEYLOGGER (THAT'S IT!)

PHISHING

"We'll trick you into clicking on a suspicious email link, then we'll steal all your stuff."



\$600,000:

NEARLY LOST IN A PHISHING SCAM AT A WISCONSIN DISTRICT⁴

TARGETS



EMAIL

From sophisticated phishing emails to malware in a Word doc.



WEB

Even sharing a post on social media can spread malware.



SYSTEMS

Thieves can crack open storage & hold copies of data for ransom.



WORKSTATIONS

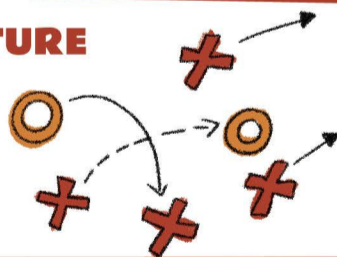
Lock it up!

DEFENSE

TRAINING, DRILLS, & CULTURE

TRY THIS:

Set up a **phishing drill** for your team.⁵



CRISIS PLANNING

(12% of businesses have one—do you?)⁷

NO PLAN? Never fear!

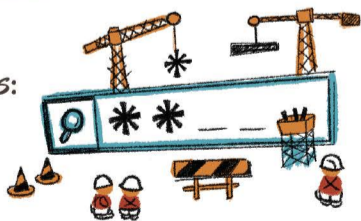
Set one up now & **save millions** in the long run.⁸



PASSWORD PROCESSES

3 WAYS kids might steal your passwords:

1. Guess it.
2. Log it.
3. Phish it.⁶



BACKUP (3-2-1)

1: Keep 3 copies of any important file

(1 primary, 2 backups) ...

2: Keep copies on 2 different media types.

3: Store 1 copy offsite.⁹

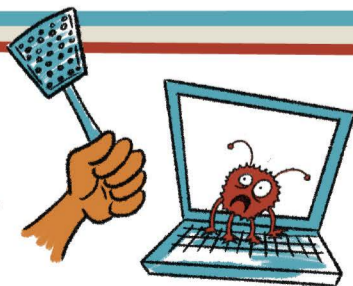


SOFTWARE

TIP:

New malware is emerging constantly...

Has your **antivirus software** been updated lately?



VPN

PROTECT your network by

connecting devices to a **virtual private network** instead of public wifi



(1) <https://bit.ly/2YvAQvB> (2) <https://wbur.fm/2YeTPyV> (3) <https://zd.net/2K5bkcq> (4) <https://bit.ly/2LOiKMD> (5) <https://bit.ly/2OqkxjD>
 (6) <https://bit.ly/2Otqahc> (7) <https://bit.ly/2Ytavhp> (8) <https://bit.ly/2KhEeor> (9) <https://bit.ly/2ZlJpP3>