vartek

Cyberattack:

One of the biggest threats to your school and what to do about it

Schools and children are top targets for cybercriminals.

“Children present unique security risks when they use a computer—not only do you have to keep them safe, you have to protect the data on your computer. By taking some simple steps, you can dramatically reduce the threats.”

—United States Computer Emergency Readiness Team

What you'll learn

1. The scope of the threat

2. Two-track defense strategy, including:

- What common cyberattacks look like and how to spot them
- What to do to protect people and systems

Scope of the Threat

2 Cyber incidents per week at U.S. schools since 2016*

14.9M School records compromised since 2005

$25M Cyber ransom paid by schools

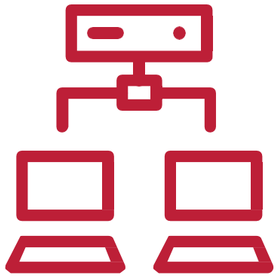
1 in 5 Cyber incidents caused by staff, students

Sources: *K12 Cybersecurity Resource Center (k12cybersecure.com)—keeps a real-time map of incidents; Education Dive; Readiness and Emergency Management for Schools Technical Assistance Center; STOP. THINK. CONNECT campaign led by the Anti-Phishing Working Group and the National Cyber Security Alliance

Two-Track Defense Strategy

Train your people.

Protect your systems.



Train your people.

Train your people.

Raise awareness.

Build new habits.

Take control.

Train your people.

vartek

Raise awareness

of common cyberattacks and how to spot them.

Cyberattackers' favorite data

- Names
- Addresses
- Social Security numbers
- Credit card numbers
- Login information (usernames, passwords, etc.)
- Account information

vartek

Cyberattackers' favorite weapons

- Phishing
- Malware
- Ransomware
- Distributed denial of service attacks

vartek

Phishing (social engineering)

A request—often for personally identifiable information or financial data—that appears to be from an organization or a person the recipient knows

Malware

Software intended to damage or disable computers and computer systems; can come from web downloads such as attached files or from clicking on internet ads

Train your people.

vartek

Ransomware

When cyber blackmailers lock up your systems and will release them only after you pay what they demand

Distributed denial of service

When a cyber criminal floods a whole network with traffic, crashing the system and preventing legitimate users from accessing email, files, and online accounts and other services.

vartek

Build new habits

that contradict what cyberattackers expect.

vartek

Beware of

- Unusual or unexpected emails—especially those that ask for money;
- A hyperlink that doesn’t match what the text says it should be; and
- Poor spelling and grammar and “URGENT” notices.

Pause and think

Before responding to email or other online prompts. Double check not only that the sender is familiar but that the message makes sense, no matter who sent it.

Take control

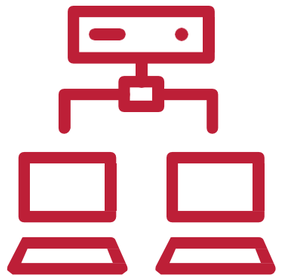
of how everyone in your school uses the internet.

vartek

Set clear standards

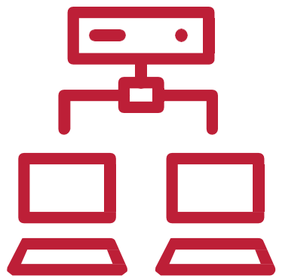
With an acceptable use policy for device and internet behavior that minimizes the risk of social engineering and cyberbullying.

vartek



Protect your systems.

Protect your systems.



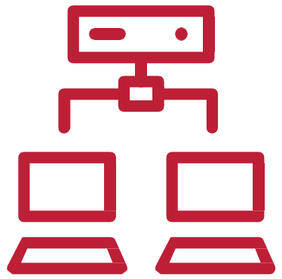
Build a fortress.

Watch carefully.

Keep tools sharp.

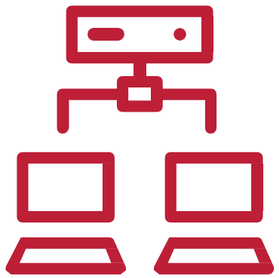
Know the signs of data compromise.

vartek



Build a fortress.

Develop policies and processes that make devices and networks less vulnerable to cyberattack.

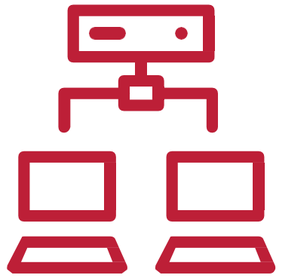


Policies & processes

- Install software patches.
- Set up firewalls.
- Create password protocols—such as required changes every ninety days.

Protect your systems.

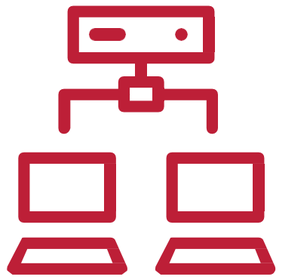
vartek



Watch carefully,

with on- and off-site software tools.

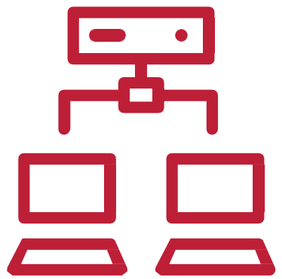
vartek



On & off-site tools

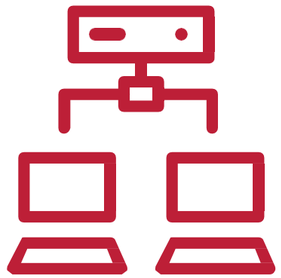
- Use remote monitoring and cloud-based backups.
- Track and manage school- and personally owned devices with a mobile device management system.

vartek



Keep tools sharp.

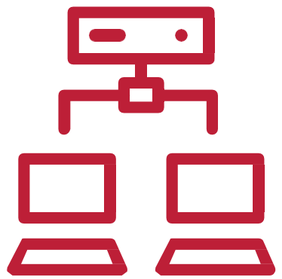
vartek



IT systems are stronger if you

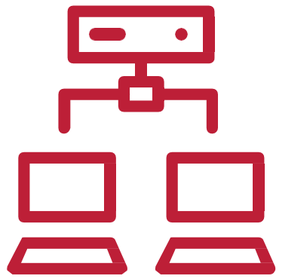
- update software regularly;
- review and set proper email security preferences; and
- retire equipment that’s too old to accommodate current security protocol.

vartek



Know the signs of data compromise.

vartek



Sometimes even fortresses have flaws.

Be on alert for key signs that a cyberattacker has succeeded despite your best efforts.

vartek

Clues to a compromise

- Problems with administrative logins and access
- Slower-than-normal network and spikes in network traffic
- Performance issues affecting the accessibility of your website
- User passwords that stop working
- Missing or altered data
- Parents and other stakeholders receiving spam from your school’s email system
- Numerous pop-up ads

In Review

- **Raise awareness:** Know the common cyberattacks and how they work.
- **Build new habits:** Don’t do what attackers expect.
- **Take control.** Set clear online behavior expectations.
- **Build a fortress.** Install firewalls and patches.
- **Watch carefully.** Use remote monitoring.
- **Keep tools sharp.** Don’t let software and hardware become obsolete.
- **Know the signs of data compromise.** Detecting it early can reduce the effects.

CoSN (Consortium for School Networking) recommends

that a school work with a strategic IT partner with the expertise to audit and manage school IT security and be on the ground to respond to a cyberattack.

Want to know more about strategic IT partnerships?

Email info@vartek.com, or call 800-954-2524.