Malware in K12

for Beginners

Welcome to our series on cybersecurity in K-12 schools! We're going on a field trip through some of the most common threats schools face — threats that hinder a safe learning environment and can have consequences for students even after they leave school. We'll talk about **what they are, how they affect schools and how to prevent them.**

Today's stop: **malware**.

jamf

IN THIS E-BOOK, WE'LL DIVE INTO MALWARE IN EDUCATION BY COVERING:

What is malware?

Malware — malicious software or firmware — is a significant threat to K-12 schools. It comes in many forms and by many means, making it a challenge to defend against. Generally, malware is used to compromise the confidentiality, integrity and/or availability of the data or applications in a system.

For example, the hacking group Vice Society targeted schools with **43 ransomware attacks between June 2022 and May 2023**. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) **explains Vice Society's method**:

1. Exploit internet-facing applications to gather compromised credentials, obtaining initial access.
2. Explore the network and identify ways to increase access to data.
3. Evade detection by disguising their malware as legitimate files.
4. Exfiltrate data.
5. Deploy ransomware, threatening to release sensitive data unless the ransom is paid.

Naturally, this is cause for concern. But schools have the power to reduce their chance of falling victim to these attacks.

Bring Security Learning to the Class

Malware combines two words: "malicious", something that is harmful, and "software", the programs that run on a computer, to mean harmful computer programs. These bad programs can do many different things, like spy on people, steal information, take over a computer or bully people into giving them money.

Lesson Ideas:

1. Have students create a sketchnote that illustrates what malware is
2. Create a rap about Malware safety

Different malware types

RANSOMWARE

Ransomware, at its core, is a form of malware in which malicious actors gain access to a user's files, encrypting them and rendering them inaccessible. To restore access, users are required to pay a ransom to the attackers. Attackers may demand payment to decrypt data and confirm they have deleted data from their systems.

TROJANS

Trojans are a type of malware that appears to be a legitimate program but in fact contains malicious code. This code could be packaged with files downloaded from the internet, including pirated or compromised legitimate software packages.

Trojans are used to create backdoors for bad actors to come in and out of a network, to exploit vulnerabilities in applications, to deliver ransomware and more. Unlike viruses and worms, trojans do not self-replicate or spread to other systems, though they could contain malware that does.

VIRUSES

Much like the viruses that make us sick and spread, malware viruses are able to self-replicate and spread to other devices upon user interaction. They lie dormant until they've been activated by a user action, making it more difficult to identify the source of the virus.

Viruses serve many purposes for bad actors, including disabling or launching certain applications, displaying popups or sending mass emails without the user knowing. They may spread through email links, attachments or online downloads to disrupt systems, cause major operational issues, and result in data loss and leakage.

Bring Security Learning to the Class

Lesson Idea:

1. Have students create a short video about a different type of malware

2. Gamify it! Create a matching game that helps students connect malware names to what it is

WORMS

Like viruses, worms have the ability to self-replicate. Unlike viruses, they can self-propagate by, well, worming their way to other devices on their own. Worms are used to create backdoors, deploy other malware, collect data, overload networks and more. They spread via phishing attack and other means of communicating or file sharing, exploiting software and network vulnerabilities.

CRYPTOJACKING

Cryptojacking — the behind-the-scenes takeover of a computer to mine cryptocurrency — is a growing threat to institutions. According to Sonicwall, the first half of 2023 saw a 320x increase in cryptojacking compared to 2022. Cryptojacking, unlike ransomware, doesn't loudly announce its existence on a device. Instead, it strains a device's computing power, reducing your system speeds by up to 70%.

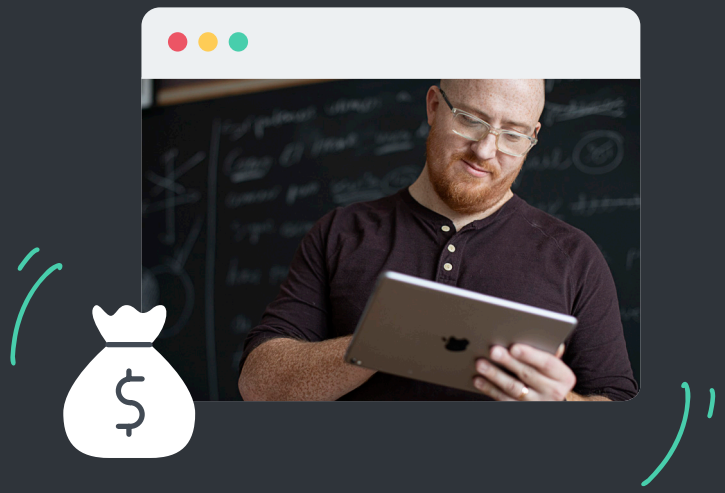
Stay tuned: later in this e-book series, we'll take a deep dive into this growing threat to schools.

SPYWARE

Spyware is malware that, well, spies on a device's activity. For example, it may record mouse movements, clicks and any action the user takes. It may be used to harvest credentials or personal information.

While not technically spyware, some schools chose to surveil students' school-issued computers with the intention to keep them focused and safe. But is this actually safer? This type of software **raises concerns for student privacy** and wellbeing without definitively providing a safer environment.

MALWARE IN K-12 SCHOOLS



80%

of lower education respondents were hit by ransomware — a 24% increase from 2022. On average, the cost to recover the data (excluding a ransom payment) was **$1.59 M.**

Malware can enter a system via a teacher, student or administrator — and data belonging to each of these groups can be compromised by malware. A **2020 data breach of the Toledo Public School System** resulted in bad actors attempting to open credit cards, taking out car loans and other similar exploits using the information of children in the school system. And a 2020 attack on one US school district included personally identifiable information (PII) for over 500,000 students and other information for more than 56,000 employees. Students, some who are years away from being able to check their credit reports or other measures, are especially in danger when it comes to their data being compromised.

Ransomware is the hot topic in education cybersecurity. This theatrical-sounding threat is unfortunately very real and very common — especially for schools. In fact, **K-12 schools are the top target** for ransomware. The Sophos publication, **The State Of Ransomware in Education 2023** reports that **80% of lower education respondents were hit by ransomware — a 24% increase from 2022. On average, the cost to recover the data (excluding a ransom payment) was $1.59 M.**

Why are schools such a hot target for ransomware?

Schools aren't always prepared with the same resources as corporations are, whether its from a lack of awareness, funds or suitable software solutions. As a result, **schools falling victim to cyber attacks experience**:

3 to **21** days of **learning lost**

Possibly **months** of recovery time

Nearly **$900,000** in **ransom** payments

(if they choose to pay the ransom)

Possible exposure of **sensitive data**

Thankfully, **most schools get their data back**.

73% used backups

47% paid the random

2% used others means

But note that that this doesn't necessarily mean their data was contained — bad actors may still have sold or otherwise distributed the data.

MALWARE PREVENTION

According to the Sophos State of Education report, ransomware attacks are primarily driven by:

- Exploited vulnerabilities
- Compromised credentials
- Malicious emails
- Phishing

Part of the battle is stopping malware attacks before they can take hold in your system. And since no defense is flawless, the other part is being able to recover with minimal impacts on learning, finances and downtime. Being attacked with malware isn't a matter of if, but of *when*. Let's focus on a handful of ways to reduce the affect of malware on your system.

While your devices and your school rules are designed to prevent malware from getting on your device, you can help prevent it too!

Here's what you can do:

1. Never share your login info with anyone.
2. Don't download files or software from the internet — make sure they are from a trusted source; ask if you aren't sure.
3. Pay attention to where a link takes you. Does the website name and appearance look like it should? If it looks suspicious, do not enter your information. It's often better to retype the website to make sure you're on the right page.
4. Keep your devices updated with the latest software.

SOFTWARE UPDATES AND DISTRIBUTION

Keeping software — both applications and operating systems — up to date can reduce the chance a vulnerability in the software will be exploited. Bad actors can create malware that targets vulnerabilities in commonly used software to escalate privileges and/or deliver additional malware.

Because online downloads — from trusted sources or not — can contain malware, restricting software downloads can help avoid trouble. Depending on how your devices are managed, there are a few options to deploy IT-approved apps to users:

- Jamf Self service portal
- App Store
- Apple School Manager
- **Via your MDM platform**

MULTIFACTOR AUTHENTICATION

Multifactor authentication (MFA) is a first line of defense to prevent compromised credentials from resulting in disaster. MFA requires two or more factors of authentication to log into an account. These factors include:

- Something you **know**, like a password or pin
- Something you **have**, like an authenticator app or hardware fob
- Something you **are**, like a fingerprint, retinal or facial scan

Devices that offer biometric authentication, like an iPad, can make it easier for younger students who may not have access to another authentication device. Schools or districts can add another line of defense by using single sign-on with MFA to limit the number of passwords students would need to remember.

BACKUPS

As hinted in earlier paragraphs, backups can make all the difference in whether or not your data is recovered in a ransomware attack. Regular backups can also provide a restore point if your systems become compromised by other types of malware. These two benefits alone make backups critical for maintaining your data's integrity and security.

Bring Security Learning to the Class

Lesson Idea:

1. Have students create a keynote presentation about a different prevention tip and why it helps keep everyone safe

DEVICE MANAGEMENT

Mobile device management (MDM) acts as a foundation to keeping devices in shape. MDM gives it admins the ability to:

- Keep an inventory of devices connected to school resources
- Determine and act upon a device's security compliance
- Update devices and their software to the latest versions
- Require certain security policies to reduce the risk of a data breach
- Restrict access to certain applications and/or websites

CONTENT FILTERING

Despite good user education, people slip up, especially on mobile devices where it's difficult to see or preview links. **Content filtering tools** can help prevent successful attacks by blocking malicious links. For example, if a student receives a well-disguised phishing email and clicks on a link intended to harvest their credentials, content filtering can block their access to that website.

SECURITY FRAMEWORKS

While not all schools or districts have the staff, finances or resources to implement and enforce the parts of a security framework they provide a goal to aspire to. Frameworks like these can help guide IT departments to the most secure configuration possible for their resources and staffing:

- **US Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials**
- **UK Cyber Essentials**
- **The IT Infrastructure Library (ITIL)**

jamf

Bring Security Learning to the Class

User education:

It's never to early to start education about cybersecurity mindfulness. Students, faculty and staff should be informed about risky behaviors, like:

- Clicking on links before considering their legitimacy
- Sharing their login credentials
- Inserting unknown USB drives or other removable media into their device
- Downloading software from third-party sites
- Not updating their devices or applications

Phishing attacks are extremely common — users should be aware of how to recognize phishing attempts. Features like these can be indicators:

- Lookalike URLs with special characters or strange formatting
- Misspellings or unusual language in emails (though attackers are creating better and better messages)
- Urgent demand for action
- Unusual and/or unsolicited messages, including from people you know

IMPLEMENTATION: JAMF SCHOOL AND JAMF SAFE INTERNET

Ok, we've talked about some ways to prevent malware. But how do we actually implement these strategies?

Jamf School

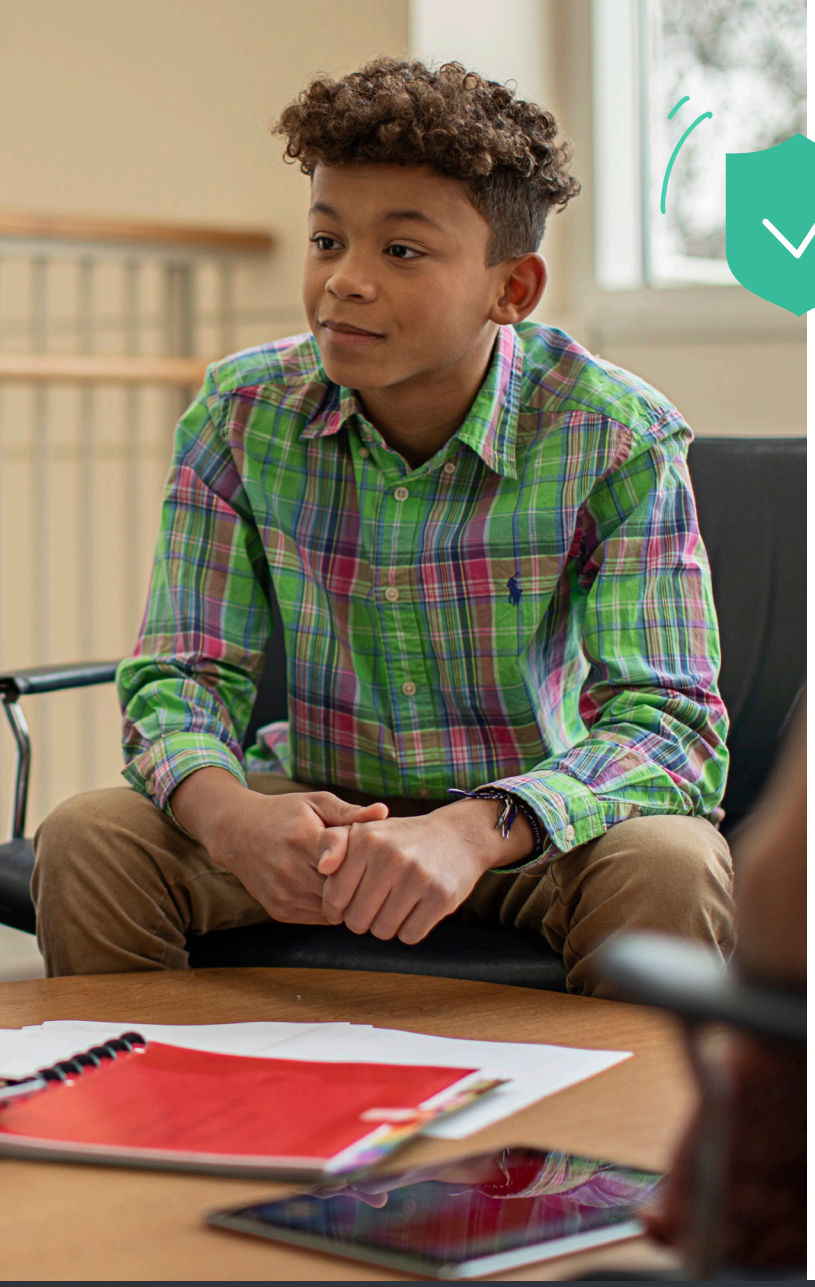
We mentioned that MDM is the foundation for keeping your devices secure. While it isn't enough on its own, it is critical as it provides necessary transparency into the devices that are interacting with student and employee data.

On some level, **management IS security.**

Jamf School is education-focused MDM for schools, making it simple to deploy, manage and secure Mac, iPad, iPhone and Apple TV. It offers:

- Transparency into managed devices, users and apps
- Simple software deployment and upgrades
- The ability to configure device security settings, including passcode policies and content filtering
- Robust and secure app deployment and updating with vetted apps
- Classroom management tools to keep learners focused

Security starts in management, knowing your devices — and what is on them — means you can support the security of the device; from updates of required software to deploying specific security controls.



IMPLEMENTATION

Jamf Safe Internet

Jamf Safe Internet goes beyond MDM to create a safe and secure learning environment by allowing students to browse privately without encountering malware or other types of dangerous content. Compatible with Apple, ChromeOS and Windows devices, Jamf Safe Internet features:

Fully customizable with the flexibility to easily set or change policies that apply to different groups based on device type, geography or other attributes. Jamf Safe Internet works with any managed device, whether it lives in a cart, was assigned by the school or is personally owned.

Powerful content filtering with:

- Enforced Google Safe Search
- YouTube Restricted Mode to show only educational content
- Advanced machine learning to detect and prevent undiscovered threats
- Real time, in-network protection to prevent access to phishing sites and other malicious domains

Security without surveillance by allowing students the freedom to explore the internet and develop digital citizenship — without violating their privacy or putting them in danger.

jamf

See how Jamf can help be a part of your technology, security, and content filtering solution

Get Started

www.jamf.com

© 2024 Jamf, LLC. All rights reserved.