Spam in K12

for Beginners

jamf

Spam in K12

for Beginners

We've been on an e-book journey through common cyber threats that K-12 schools face every day. Our field trip has taken us through:

- **Malware**
- **Phishing**
- **Cryptojacking**

This time, we're going to talk about spam. It isn't always malicious, but it can leave us feeling pretty salty — and it can be a real obstacle to learning.

IN THIS E-BOOK, WE'LL DIVE INTO SPAM IN EDUCATION BY ANSWERING:

1. What is spam?
2. What forms does spam come in?
3. How does Spam affect K-12 users?
4. How do you prevent spam?

What is spam?

Generally, spam is unwanted, unsolicited, bothersome content used for advertising, obtaining information or spreading malware. This could be emails, phone calls, text messages, messages on social media and more. While spam isn't always malicious, it certainly can be, causing more than just annoyance to the recipient.

You may have heard of an example, where U.S. students received targeted racist text messages. While these messages aren't necessarily cyber threats (that is, intending to steal information), they certainly cause upset and discord.

This isn't the first time spam has disrupted students. In 2020, middle and high schoolers in Florida received "millions of spam emails containing offensive and inappropriate content," in this case more racist messaging and sexually explicit messages about a school employee.

Spam messages can also be crafted to deceive—whether they're phishing for your personal information, scheming to get money, or pulling off another con.

It's not difficult to imagine how spam could negatively affect students, whether it's by:

- Alienating certain populations
- Exposing children to disturbing or inappropriate content they may not know how to process
- Disrupting lessons as students discuss the contents
- Cluttering inboxes with unnecessary messages
- Capitalizing on student naiveté for financial or other gain

What forms does spam come in?

Spam comes in all kinds of forms, and is constantly evolving to capture the most victims. You might come across spam in:

Emails **Text messages** **Forum posts** **Voice calls** **Social media**

While the exact form of the spammy message varies, they tend to follow some patterns, which we'll talk about now.

Inappropriate content

Like the examples we mentioned before, spam can aim to upset or shock the recipient. While the intent of these messages isn't always clear, they can cause disruption. Recipients could feel hurt or discouraged by these messages. Or it disrupt learning if students are talking about the messages during a lesson, for example.

Advertising

Unsolicited messages from a legitimate organization inviting users to buy their product is still considered spam. For example, a student receives a message saying they can "get exclusive discounts if they make a purchase before midnight!" While this isn't necessarily harmful, it wastes a student's time and takes up space in their inbox.

Malware and phishing

Some spam is intentionally created to force users to perform some action that ultimately harms them. This could be an email with a malicious file attached that once downloaded and opened, installs malware on their computer. Or it could be a message urging a user to take immediate action (implying there will be consequences if they don't), that takes them to a phishing website.

"Too good to be true" offers

Often, spam will come in the form of a "too good to be true" offer, aiming to entice the user to click on a link and give their information. This could be something like:

- Offering prize money and asking for a user's address or for a deposit
- Telling the user they won a free game console, again asking for information
- Telling the user they've been selected to be an influencer while providing a link to farm their information

Students, especially young ones, are more susceptible to this tactic.

How does Spam affect K-12 users?

Worst case scenario, spam is malicious and results in a data breach for your school. Better but still not great, is that it's simply irritating.

Best, of course, is that your security tools make sure it doesn't get in front of users at all.

Whatever the case may be, spam isn't something that can be ignored — it can have real impact on student learning. For instance, California schools received threatening spam emails containing a bomb threat. While the threats turned out to be empty, multiple schools decided to close out of an abundance of caution.

Thankfully, the consequences of these emails didn't involve catastrophe. But they affected students' learning outcomes and their general attitude toward their safety. After all, they can't learn when their classes get canceled. Students want to feel like their school is is a safe place where they can thrive and learn — spam emails compromise this.

Spam that contains phishing links or malware are destructive too. Educational institutions are hot targets for attackers. Spam can be the starting point to problems like ransomware attacks — in fact, according to the Sophos State of Ransomware in Education 2024 report, malicious emails and phishing were involved in 26% and 8% of ransomware attacks, respectively. This can result in:

- Lost learning when systems become locked down
- Data breaches where student and faculty data becomes exposed
- Expensive and time-consuming recovery

How do you prevent spam?

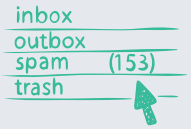
Thankfully, fighting against spam isn't a lost cause. Let's go through some tools and tactics that help prevent spam from wreaking havoc.

Mobile device management

Mobile device management (MDM) is the foundation for making sure your school's devices are configured correctly and secure. MDM makes it possible to:

- Keep track of devices, users and apps
- Log device incidents
- Deploy apps per teacher requests
- Securely configure devices

In other words, MDM gives admins the transparency into devices that they need to keep these devices operational and protected, without violating student privacy.



Email filtering

Email is a popular destination for spam, so it's critical to prevent it from ever getting in front of users. Email filters can catch spam based on their contents, sender or other attributes.

Content filtering

Not all spam comes through email, nor does any spam filter catch all spam. Content filtering is your next line of defense — it prevents users from accessing malicious or risky websites. If a student clicks on a phishing link, content filtering will block the website designed to steal their information. Content filtering can also prohibit access to social media or online forums that contain spammy material.

Security software

What happens if a user downloads malware from a spam email? Your security software can prevent this from executing and take actions necessary once malware is detected. Your security software should work with your MDM to remediate the issue.

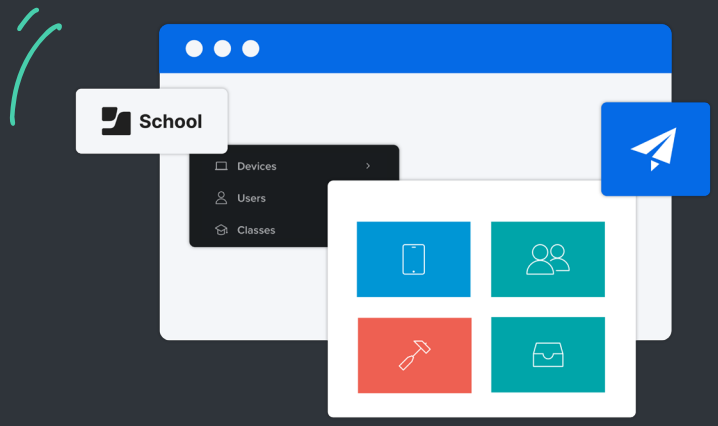
User education

User education can go a long way in preventing spam from affecting the learning experience. Teaching students, faculty and staff what to look for and what to do if they suspect something is spam is a crucial piece of the security puzzle.

IMPLEMENTATION: JAMF SCHOOL AND JAMF SAFE INTERNET

We've talked about some strategies to fight against spam — now let's talk implementation.

Jamf offers powerful software to block spam and other security threats.



Jamf School

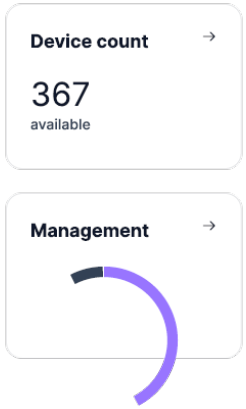
Jamf School is MDM built specifically for schools, and is designed to support learning — from the IT helpdesk to the classroom. As mentioned earlier, MDM is the cornerstone of security; Jamf School does MDM to meet education requirements.

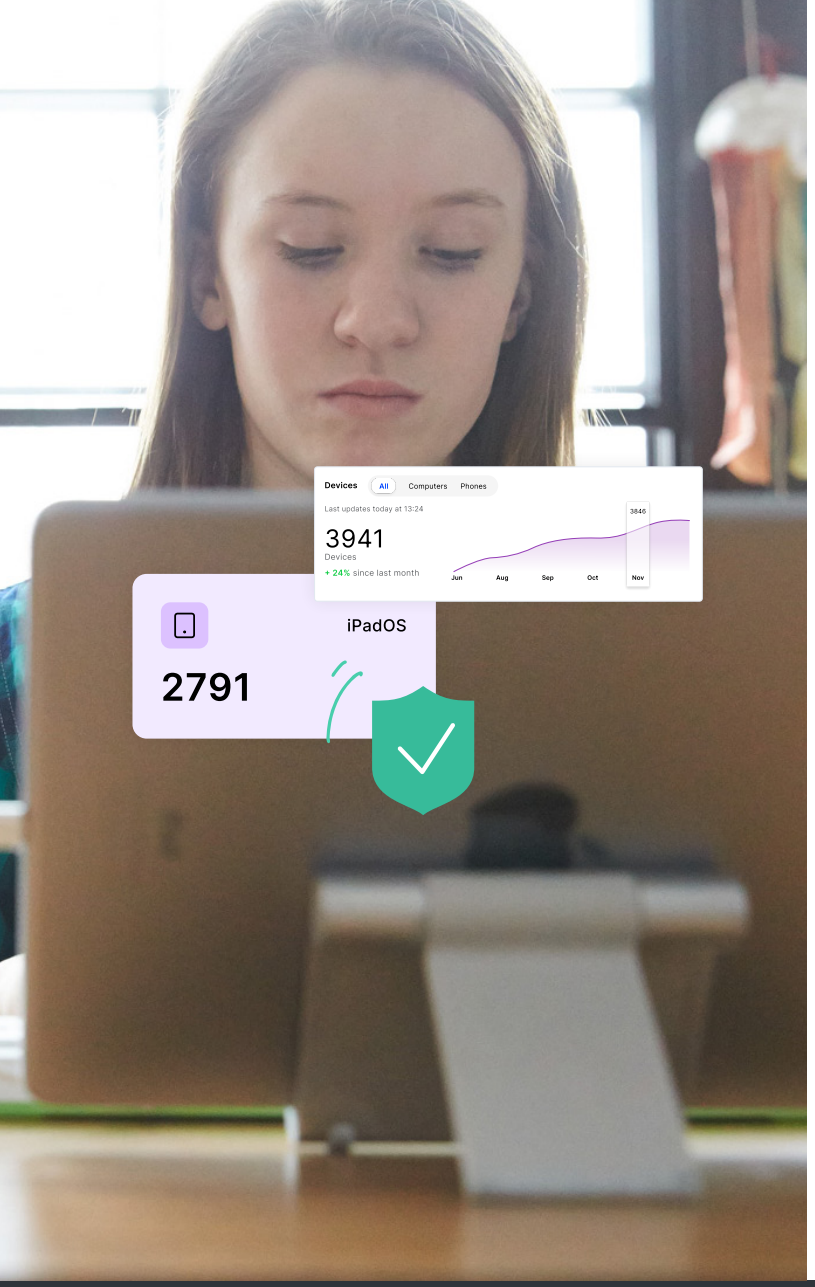
Jamf School helps manage devices through:

- Dashboards to keep track of managed devices, apps and users
- Making it easy to drag and drop apps, content and restrictions
- Keeping track of device damage and incidents

Free, included apps like Jamf Teacher are designed to be used in the classroom: if students are distracted, have questions, or come across spam or other troubling content, teachers can quickly address any issues by:

- Displaying an alert on student devices
- Messaging back and forth with students
- Restricting access to certain websites and/or apps





Jamf Safe Internet

The internet has so much to offer — sadly, including spam, malware and phishing. Jamf Safe Internet's powerful network threat prevention and content filtering is designed to protect students from these threats. This content filtering works on device, meaning students don't have to be on a school's Wi-Fi for it to work.

Beyond malicious websites, admins can block other categories, like entertainment, games and social media. Additionally, Jamf Safe Internet enforces Google SafeSearch and YouTube Restricted Mode to ensure content stays appropriate.

Jamf Safe Internet prevents attackers from stealing personal information; personal information should stay private. That's why Jamf Safe Internet works without violating student privacy by surveilling their actions.

jamf

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

Get Started

www.jamf.com