Spam in K12

für Einsteiger:innen

jamf

Spam in K12

für Einsteiger:innen

Wir haben uns auf eine E-Book-Reise durch gängige Cyberbedrohungen begeben, mit denen Grund- und weiterführende Schulen (K12) tagtäglich konfrontiert sind. Unsere Exkursion hat sich mit folgenden Themen beschäftigt:

- **Malware**
- **Phishing**
- **Kryptojacking**

Dieses Mal geht es um Spam. Das ist nicht immer bösartig, aber es kann ein unangenehmes Gefühl hinterlassen – und ein echtes Lernhindernis darstellen.

IN DIESEM E-BOOK BEFASSEN WIR UNS MIT MALWARE IM BILDUNGSBEREICH:

1. Was Spam ist?
2. In welchen Formen er auftritt?
3. Wie er Benutzer:innen grund- und weiterführender Schulen (K12) betrifft?
4. Was man dagegen tun kann?

Was ist Spam?

Im Allgemeinen handelt es sich bei Spam um unerwünschte, unaufgeforderte, lästige Inhalte, die für Werbung, Informationsbeschaffung oder die Verbreitung von Malware genutzt werden. Dies können E-Mails, Telefonanrufe, Textnachrichten, Nachrichten in Sozialen Medien und mehr sein. Auch wenn Spam nicht immer bösartig ist, kann er doch mehr als nur ein Ärgernis für den Empfänger sein.

Vielleicht haben Sie schon von einem Beispiel gehört, bei dem Schüler:innen in den USA gezielt rassistische Textnachrichten erhielten. Auch wenn es sich bei diesen Nachrichten nicht unbedingt um Cyberbedrohungen handelt (d. h. die Absicht, Informationen zu stehlen), sorgen sie doch für Unruhe und Unfrieden.

Es ist nicht das erste Mal, dass Schüler:innen durch Spam gestört werden. Im Jahr 2020 erhielten Mittel- und Oberschüler:innen in Florida "Millionen von Spam-E-Mails mit beleidigenden und unangemessenen Inhalten", in diesem Fall rassistische Botschaften und sexuell eindeutige Nachrichten über eine Mitarbeiterin der Schule.

Auch Spam-Nachrichten können darauf abzielen, zu täuschen, sei es durch Phishing nach persönlichen Informationen, durch den Versuch, an Geld zu kommen oder durch etwas anderes.

Es ist nicht schwer, sich vorzustellen, wie sich Spam negativ auf Schüler:innen auswirken könnte, sei es durch:

- Entfremdung bestimmter Bevölkerungsgruppen
- Kinder beunruhigenden oder unangemessenen Inhalten aussetzen, die sie möglicherweise nicht verarbeiten können
- Fortschritt im Unterricht wird unterbrochen, wenn Schüler:innen über den Inhalt diskutieren
- Überfüllung der Posteingänge mit unnötigen Nachrichten
- Ausnutzen der Naivität von Schüler:innen zu finanziellen oder anderen Zwecken

Welche Formen von Spam gibt es?

Spam gibt es in allen möglichen Formen, und er wird ständig weiterentwickelt, um die meisten Opfer zu erreichen. Sie könnten auf Spam stoßen:

E-Mails | **Textnachrichten** | **Forum-Beiträge** | **Sprachanrufe** | **Soziale Medien**

Auch wenn die genaue Form der Spam-Nachricht variiert, folgen sie in der Regel einigen Mustern, auf die wir jetzt eingehen werden.

Unangemessener/ umwerfender Inhalt

Wie die zuvor erwähnten Beispiele kann auch Spam darauf abzielen, den Empfänger zu verärgern oder zu schockieren. Obwohl die Absicht dieser Nachrichten nicht immer klar ist, können sie Störungen verursachen. Die Empfänger könnten sich durch diese Nachrichten verletzt oder entmutigt fühlen. Oder es stört das Lernen, wenn Schüler:innen zum Beispiel während des Unterrichts über die Nachrichten sprechen.

Werbung

Unaufgeforderte Nachrichten von einer seriösen Organisation, die Benutzer:innen zum Kauf ihres Produkts auffordert, gelten immer noch als Spam. Zum Beispiel erhält eine Schüler:in eine Nachricht, die besagt, dass sie "exklusive Rabatte erhalten kann, wenn sie vor Mitternacht einen Kauf tätigt!" Das ist zwar nicht unbedingt schädlich, aber es verschwendet die Zeit der Schüler:innen und nimmt Platz in ihrem Posteingang ein.

Malware und Phishing

Manche Spam-Mails werden absichtlich erstellt, um Benutzer:innen zu einer Aktion zu zwingen, die ihnen letztlich schadet. Dabei kann es sich um eine E-Mail mit einer bösartigen Datei im Anhang handeln, die, sobald sie heruntergeladen und geöffnet wurde, Malware auf ihrem Computer installiert. Oder es handelt sich um eine Nachricht, die Benutzer:innen zu sofortigen Aktionen auffordert (und ihnen andernfalls Konsequenzen androht) und sie auf eine Phishing-Website führt.

"Zu schön, um wahr zu sein" - Angebote

Oft wird Spam in Form eines "zu schön, um wahr zu sein"-Angebots versendet, das Benutzer:innen dazu verleiten soll, auf einen Link zu klicken und ihre Daten anzugeben. Dies könnte etwa so aussehen:

- Auslobung von Preisgeldern mit der Bitte um die Adresse eines/r Benutzer:in oder um eine Einzahlung
- Der/die Benutzer:in wird mitgeteilt, dass er/sie eine kostenlose Spielkonsole gewonnen hat, und es wird erneut nach Informationen gefragt
- Dem/der Benutzer:in wird mitgeteilt, dass er/sie als Influencer ausgewählt wurde, und es wird ein Link zum Farmen seiner/ihrer Informationen bereitgestellt

Schüler:innen, insbesondere junge, sind für diese Taktik besonders anfällig.

Spam in Grund- und weiterführenden Schulen (K12)

Im schlimmsten Fall ist der Spam bösartig und führt zu einer Verletzung der Daten Ihrer Schule. Besser, aber immer noch nicht großartig, ist, dass es einfach irritierend ist.

Am besten ist es natürlich, wenn Ihre Sicherheitstools dafür sorgen, dass sie den Benutzer:innen gar nicht erst unter die Augen kommen.

Wie dem auch sei, Spam kann nicht einfach ignoriert werden - es kann echte Auswirkungen auf das Lernen der Schüler:innen haben. So erhielten beispielsweise kalifornische Schulen bedrohliche Spam-E-Mails mit einer Bombendrohung. Obwohl sich die Bedrohungen als unbegründet herausstellten, beschlossen mehrere Schulen, aus Vorsicht zu schließen.

Glücklicherweise hatten diese E-Mails keine katastrophalen Folgen. Aber sie wirkten sich auf die Lernergebnisse der Schüler:innen und ihre allgemeine Einstellung zu ihrer Sicherheit aus. Schließlich können sie nicht lernen, wenn ihre Klassen ausfallen. Schüler:innen wollen das Gefühl haben, dass ihre Schule ein sicherer Ort ist, an dem sie sich entfalten und lernen können - Spam-E-Mails gefährden dies.

Auch Spam, der Phishing-Links oder Malware enthält, ist schädlich. Bildungseinrichtungen sind ein beliebtes Ziel von Angreifern. Spam kann der Ausgangspunkt für Probleme wie Ransomware-Angriffe sein - laut dem Sophos State of Ransomware in Education 2024 Report waren bösartige E-Mails und Phishing in 26 % bzw. 8 % der Ransomware-Angriffe involviert. Dies kann folgende Konsequenzen haben:

- Verlorenes Lernen, wenn Systeme blockiert werden
- Datenschutzverletzungen, bei denen Daten von Schüler:innen und Lehrkräften aufgedeckt werden
- Teure und zeitaufwändige Wiederherstellung

Spam-Abwehr

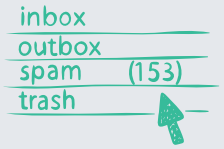
Zum Glück ist der Kampf gegen Spam noch nicht verloren. Gehen wir einige Tools und Taktiken durch, die verhindern, dass Spam verheerenden Schaden anrichtet.

Mobile Device Management (Mobilgeräteverwaltung, MDM)

Die Mobilgeräteverwaltung (MDM) ist die Grundlage, um sicherzustellen, dass die Geräte Ihrer Schule korrekt und sicher konfiguriert sind. MDM macht es möglich:

- Behalten Sie den Überblick über Geräte, Benutzer:innen und Apps
- Einloggen von Vorfällen am Gerät
- Bereitstellen von Apps auf Anfrage von Lehrkräften
- Sichere Konfiguration von Geräten

Mit anderen Worten: MDM verschafft den Admins die Transparenz über die Geräte, die sie benötigen, um diese Geräte betriebsbereit und geschützt zu halten, ohne den Datenschutz der Schüler:innen zu verletzen.



E-Mail-Filterung

E-Mails sind ein beliebtes Ziel für Spam, daher muss verhindert werden, dass diese jemals vor die Augen der Benutzer:innen gelangen. E-Mail-Filter können Spam aufgrund des Inhalts, des Absenders oder anderer Attribute abfangen.

Filterung von Inhalten

Nicht jeder Spam kommt per E-Mail, und kein Spamfilter fängt alle Spams ab. Die Filterung von Inhalten ist Ihre nächste Verteidigungslinie - sie verhindert, dass Benutzer:innen Zugang zu bösartigen oder riskanten Websites erhalten. Wenn eine Schüler:in auf einen Phishing-Link klickt, blockiert die Filterung von Inhalten die Website, auf der ihre Daten gestohlen werden sollen. Die Filterung von Inhalten kann auch den Zugang zu Sozialen Medien oder Online-Foren verhindern, die spammiges Material enthalten.

Sicherheitssoftware

Was passiert, wenn eine Benutzer:in Malware aus einer Spam-E-Mail herunterlädt? Ihre Sicherheitssoftware kann die Ausführung verhindern und die notwendigen Aktionen durchführen, sobald Malware erkannt wird. Ihre Sicherheitssoftware sollte mit Ihrem MDM zusammenarbeiten, um das Problem zu beheben.

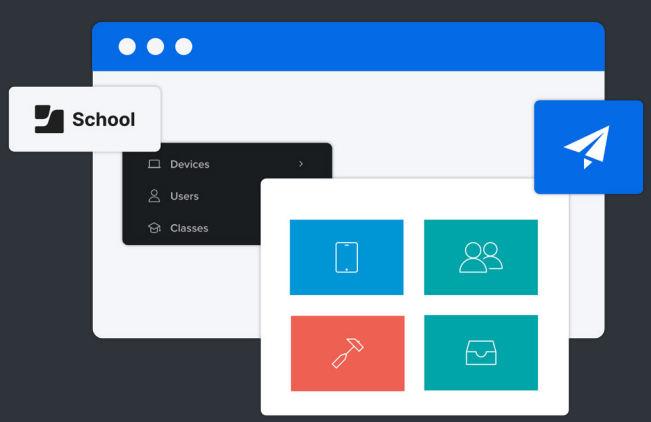
Benutzerschulung

Die Bildung der Benutzer:innen kann einen großen Beitrag dazu leisten, dass Spam das Lernerlebnis nicht beeinträchtigt. Schülern:innen, Lehrkräften und Mitarbeiter:innen beizubringen, worauf sie achten müssen und was zu tun ist, wenn sie den Verdacht haben, dass es sich um Spam handelt, ist ein wichtiger Teil des Sicherheitspuzzles.

IMPLEMENTIERUNG: JAMF SCHOOL UND JAMF SAFE INTERNET

Wir haben über einige Strategien zur Bekämpfung von Spam gesprochen - jetzt geht es an die Umsetzung.

Jamf Angebote bietet eine leistungsstarke Software zum Blockieren von Spam und anderen Bedrohungen der Sicherheit.



Jamf School

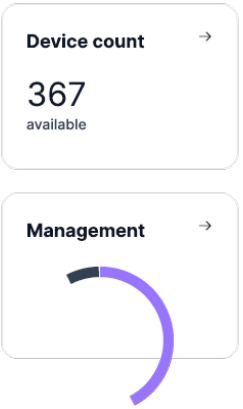
Jamf School ist ein MDM, das speziell für Schulen entwickelt wurde und das Lernen unterstützt - vom IT-Helpdesk bis zum Klassenraum. Wie bereits erwähnt, ist MDM der Eckpfeiler der Sicherheit; Jamf School führt MDM durch, um die Sicherheitsanforderungen zu erfüllen.

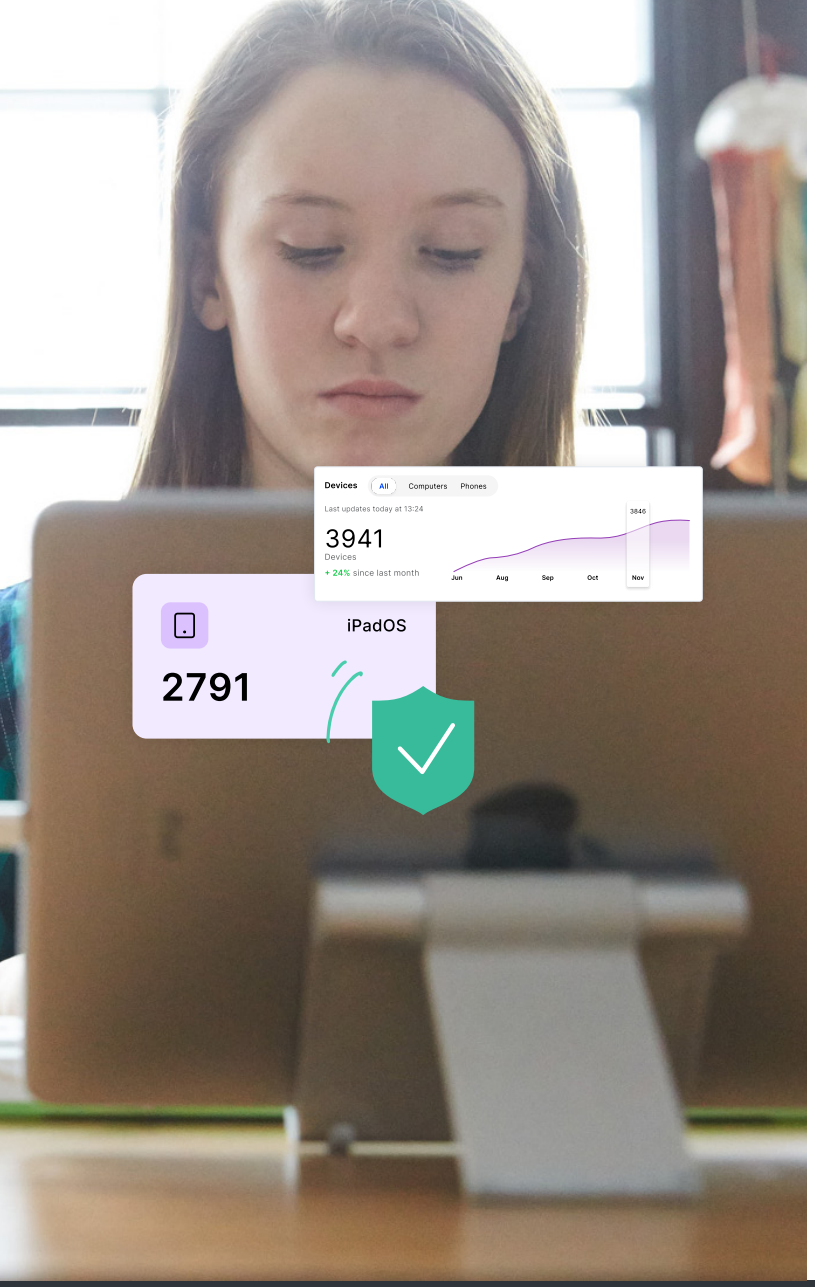
Jamf School hilft bei der Geräteverwaltung anhand von:

- Dashboards, um den Überblick über verwaltete Geräte, Apps und Benutzer:innen zu behalten
- Einfachem Ziehen und Ablegen von Apps, Inhalten und Beschränkungen
- Verfolgung von Schäden und Vorfällen am Gerät

Kostenlose Apps wie Jamf Teacher sind für den Einsatz im Klassenraum konzipiert: Wenn Schüler:innen abgelenkt sind, Fragen haben oder auf Spam oder andere bedenkliche Inhalte stoßen, können Lehrkräfte schnell auf die Probleme reagieren:

- Anzeige einer Warnmeldung auf Geräten
- von Schüler:innen
- Nachrichtenaustausch mit Schüler:innen
- Beschränkung des Zugangs zu bestimmten Websites und/oder Apps





Jamf Safe Internet

Das Internet hat so viel zu bieten - leider auch Spam, Malware und Phishing. Die leistungsstarke Netzwerk Threat Prevention und Filterung von Inhalten von Jamf Safe Internet soll Schüler:innen vor diesen Bedrohungen schützen. Diese Filterung von Inhalten funktioniert auf dem Gerät, d. h. die Schüler:innen müssen sich nicht im WLAN der Schule befinden, damit sie funktioniert.

Neben bösartigen Websites können Admins auch andere Kategorien wie Unterhaltung, Spiele und Soziale Medien sperren. Außerdem setzt Jamf Safe Internet Google SafeSearch und den Eingeschränkten Modus von YouTube ein, um sicherzustellen, dass die Inhalte angemessen bleiben.

Jamf Safe Internet hindert Angreifer daran, persönliche Informationen zu stehlen; persönliche Informationen sollten privat bleiben. Deshalb funktioniert Jamf Safe Internet, ohne den Datenschutz der Schüler:innen zu verletzen, indem ihre Aktionen überwacht werden.

jamf

Sehen Sie, wie Jamf ein Teil Ihrer Technologie-, Sicherheits- und Content-Filter-Lösung sein kann

Erste Schritte

www.jamf.com/de/