Malware in Schulen

für Beginner

Willkommen zu unserer Serie „Cybersicherheit in Schulen“!
Wir beschäftigen uns mit einigen der häufigsten Bedrohungen, denen Schulen ausgesetzt sind — Bedrohungen, die ein sicheres Lernumfeld behindern und für die Schüler auch nach dem Verlassen der Schule Folgen haben können. Wir werden darüber sprechen, **was sie sind, in welchem Umfang Schulen betroffen sind und wie man sie verhindern kann.**

Heutiges Thema: **Malware**.

jamf

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

Was ist Malware?

Malware — eine bösartige Software oder Firmware — stellt eine erhebliche Bedrohung für Schulen dar. Es gibt sie in vielen Formen und Varianten, sodass es schwierig ist, sich dagegen zu schützen. Im Allgemeinen wird Malware eingesetzt, um die Diskretion, Integrität und/oder Verfügbarkeit von Daten oder Anwendungen in einem System zu kompromittieren.

So hat beispielsweise die Hackergruppe Vice Society **zwischen Juni 2022 und Mai 2023 43 Ransomware-Angriffe** auf Schulen durchgeführt. Die US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) **hat die Methode der Vice Society erläutert**:

1. Sie nutzen internetfähige Apps aus, um kompromittierte Anmeldedaten zu sammeln und sich so einen ersten Zugang zu verschaffen.
2. Sie durchsuchen das Netzwerk und suchen nach weiteren Möglichkeiten, um den Zugang zu Daten zu erhöhen.
3. Sie umgehen die Erkennung, indem sie ihre Malware als legitime Dateien tarnen.
4. Sie exfiltrieren Daten.
5. Sie setzen Ransomware ein und drohen damit, sensible Daten freizugeben, wenn kein Lösegeld gezahlt wird.

Das gibt natürlich Anlass zur Sorge. Aber die Schulen haben es selbst in der Hand, das Risiko, Opfer solcher Angriffe zu werden, zu verringern.

Besprechen Sie das Thema Sicherheit mit der Klasse

Malware setzt sich aus zwei Wörtern zusammen: „bösartig“, etwas, das schädlich ist, und „Software“, die Programme, die auf einem Computer laufen, um schädliche Computerprogramme zu erfassen. Diese bösartigen Programme können viele verschiedene Dinge tun, z. B. Menschen ausspionieren, Informationen stehlen, einen Computer übernehmen oder Menschen dazu zwingen, Lösegeld zu zahlen.

Ideen für den Unterricht:

1. Lassen Sie die Schülerinnen und Schüler eine Sketchnote erstellen, die veranschaulicht, was Malware ist

2. Erstellen Sie eine Übersicht über Malware-Sicherheit

Verschiedene Malware-Typen

RANSOMWARE

Bei Ransomware handelt es sich im Kern um eine Form von Malware, bei der sich böswillige Akteure Zugang zu den Dateien eines Benutzers verschaffen, sie verschlüsseln und unzugänglich machen. Um den Zugang wiederherzustellen, müssen die Benutzer*innen den Cyberkriminellen ein Lösegeld zahlen. Die Kriminellen verlangen Lösegeld, um die Daten wieder zu entschlüssen und zu bestätigen, dass sie Daten von ihren Systemen gelöscht haben.

TROJANER

Trojaner sind eine Art von Malware, die vorgeben, ein legitimes Programm zu sein, in Wirklichkeit aber bösartigen Code enthält. Dieser Code könnte in Dateien enthalten sein, die aus dem Internet heruntergeladen wurden, einschließlich raubkopierter oder gefährdeter legitimer Softwarepakete.

Trojaner werden verwendet, um Hintertüren zu schaffen, durch die böswillige Akteure in ein Netzwerk eindringen und es wieder verlassen können. Die Cyberkriminellen suchen dann nach Schwachstellen in Anwendungen, um Ransomware zu verbreiten und vieles mehr. Im Gegensatz zu Viren und Würmern vermehren sich Trojaner nicht von selbst und dringen auch nicht in andere Systeme ein, obwohl sie Malware enthalten können, die dies tut.

VIREN

Ähnlich wie die Viren, die uns krank machen und sich ausbreiten, sind Malware-Viren in der Lage, sich selbst zu replizieren und sich durch Benutzerinteraktion auf andere Geräte zu übertragen. Sie schlummern, bis sie durch eine Benutzeraktion aktiviert werden, was die Identifizierung der Virenquelle erschwert.

Viren dienen böswilligen Akteuren zu vielen Zwecken, z. B. zum Deaktivieren oder Starten bestimmter Anwendungen, zum Anzeigen von Popup-Fenstern oder zum Versenden von Massen-E-Mails, ohne dass der Benutzer davon weiß. Sie können sich über E-Mail-Links, Anhänge oder Online-Downloads verbreiten und so Systeme stören, größere betriebliche Probleme verursachen und zu Datenverlusten und -lecks führen.

Besprechen Sie das Thema Sicherheit mit der Klasse

Idee für den Unterricht:

1. Lassen Sie die Schülerinnen und Schüler ein kurzes Video über eine andere Art von Malware erstellen

2. Machen Sie es zum Spiel! Machen Sie ein Spiel, das den Schüler*innen hilft, die Namen von Malware den entsprechenden Erklärungen zu den Begriffen zuzuordnen

WÜRMER

Wie Viren haben auch Würmer die Fähigkeit, sich selbst zu vermehren. Anders als Viren können sie sich selbst verbreiten, indem sie sich ihren Weg zu anderen Geräten bahnen. Würmer werden eingesetzt, um Hintertüren zu schaffen, andere Malware zu installieren, Daten zu sammeln, Netzwerke zu überlasten und vieles mehr. Sie verbreiten sich über Phishing-Angriffe und andere Kommunikationsmittel oder den Austausch von Dateien, indem sie Schwachstellen in der Software und in Netzwerken ausnutzen.

KRYPTOJACKING

Cryptojacking - die Übernahme eines Computers, um Kryptowährungen zu schürfen, ohne dass der Besitzer davon weiß - ist eine wachsende Bedrohung für Institutionen. Laut Sonicwall gab es in der ersten Jahreshälfte 2023 einen 320-fachen Anstieg von Kryptojacking im Vergleich zu 2022. Cryptojacking kündigt im Gegensatz zu Ransomware seine Existenz auf einem Gerät nicht lautstark an. Stattdessen belastet es die Rechenleistung eines Geräts und reduziert die Systemgeschwindigkeit um bis zu 70 %.

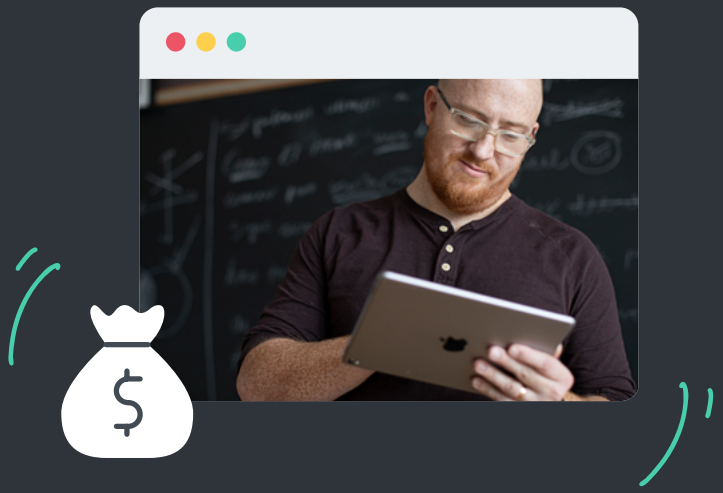
Bleiben Sie dran: Im weiteren Verlauf dieser E-Book-Reihe werden wir diese wachsende Bedrohung für Schulen genauer unter die Lupe nehmen.

SPYWARE

Spyware ist Malware, die die Aktivitäten eines Geräts ausspioniert. So können zum Beispiel Mausbewegungen, Klicks und alle Aktionen des Benutzers aufgezeichnet werden. Sie kann dazu verwendet werden, Anmeldedaten oder persönliche Informationen zu sammeln.

Obwohl es sich technisch gesehen nicht um Spyware handelt, haben sich einige Schulen dazu entschlossen, die Computer der Schüler*innen zu überwachen, damit sie fokussiert und geschützt sind. Aber ist das wirklich sicherer? Diese Art von Software **kann die Privatsphäre** und das Sicherheitsgefühl der Schüler*innen beeinträchtigen, ohne wirklich ein sichereres Umfeld zu schaffen.

MALWARE IN SCHULEN



80 %

der Befragten aus dem unteren Bildungsbereich waren von Ransomwarebetroffen – ein Anstieg um 24 % gegenüber 2022. Im Durchschnitt betrugen die Kosten für die Wiederherstellung der Daten (ohne Lösegeldzahlung) **1,59 Mio.** USD.

Malware kann über eine Lehrkraft, einen Schüler oder einen Administrator in ein System eindringen — und die Daten jeder dieser Gruppen können durch Malware gefährdet werden. Eine **Datenpanne im öffentlichen Schulsystem von Toledo im Jahr 2020** führte dazu, dass böswillige Täter versuchten, mit den Daten der Kinder des Schulsystems Kreditkarten zu beantragen, Autokredite aufzunehmen und andere ähnliche Dinge zu tun. Und bei einem Angriff auf einen US-Schulbezirk im Jahr 2020 wurden personenbezogene Daten von mehr als 500.000 Schüler*innen und Informationen von mehr als 56.000 Mitarbeiter*innen gehackt. Studierende, denen es jahrelang nicht möglich ist, eine Kreditauskunft zu beantragen oder andere Maßnahmen zu ergreifen, sind besonders gefährdet, wenn ihre Daten kompromittiert werden.

Ransomware ist ein heißes Thema im Bereich der Cybersicherheit im Bildungswesen. Diese theatralisch anmutende Bedrohung ist leider sehr real und sehr häufig - insbesondere in Schulen. Tatsächlich **sind Schulen das Hauptziel** für Ransomware. In der Sophos-Publikation **The State Of Ransomware in Education 2023** wird dargestellt, dass **80 % der Befragten aus dem unteren Bildungsbereich von Ransomware betroffen waren - ein Anstieg um 24 % gegenüber 2022. Im Durchschnitt betrugen die Kosten für die Wiederherstellung der Daten (ohne Lösegeldzahlung) 1,59 Mio. USD.**

Warum sind Schulen ein so beliebtes Ziel für Ransomware?

Schulen sind nicht immer mit den gleichen Ressourcen ausgestattet wie Unternehmen, sei es aufgrund mangelnder Aufklärung, Geldmitteln oder geeigneten Softwarelösungen. Dies hat zur Folge, dass **Schulen Opfer von Cyberangriffen werden**:

3 bis **21** Tage **Lernausfall**

Möglicherweise **Monate** für die Wiederherstellung

Fast **900.000 Dollar** an **Lösegeldzahlungen**

(falls sie sich entscheiden, das Lösegeld zu zahlen)

Mögliche Offenlegung **sensibler Daten**

Zum Glück **bekommen die meisten Schulen ihre Daten zurück**.

73 % verwendeten Backups

47 % zahlten das Lösegeld

2 % benutzten andere Methoden

Dies bedeutet jedoch nicht zwangsläufig, dass die Daten unter Verschluss gehalten wurden. Die Cyberkriminellen könnten die Daten immer noch verkauft oder anderweitig verbreitet haben.

MALWARE-PRÄVENTION

Laut dem Sophos State of Education Report werden Ransomware-Angriffe vor allem durch folgende Faktoren ausgelöst:

- Ausnutzung von Schwachstellen
- Kompromittierte Anmeldedaten
- Bösartige E-Mails
- Phishing

Ein Teil der Abwehr besteht darin, Malware-Angriffe zu stoppen, bevor sie sich in Ihrem System festsetzen können. Und da keine Verteidigung fehlerfrei ist, besteht der andere Teil darin, die Daten mit minimalen Beeinträchtigungen für das Lernen, die Finanzen und die Ausfallzeiten wiederherzustellen. Ein Malware-Angriff ist nicht eine Frage des Ob, sondern des *Wann*. Wir wollen uns nun auf eine Handvoll Möglichkeiten konzentrieren, um die Auswirkungen von Malware auf Ihr System zu verringern.

Ihre Geräte und die Schulregeln sollen zwar verhindern, dass Ihr Gerät mit Malware infiziert wird, aber auch Sie können aktiv dazu beitragen, dies zu verhindern!

Das können Sie tun:

1. Geben Sie Ihre Anmeldedaten niemals an Dritte weiter.

2. Laden Sie keine Dateien oder Software aus dem Internet herunter. Vergewissern Sie sich, dass sie von einer vertrauenswürdigen Quelle stammen; fragen Sie nach, wenn Sie sich nicht sicher sind.

3. Achten Sie darauf, wohin ein Link Sie führt. Sehen der Name und das Erscheinungsbild der Website so aus, wie es sein sollte? Wenn es verdächtig aussieht, geben Sie Ihre Daten nicht ein. Oft ist es besser, die Website erneut aufzurufen, um sicherzugehen, dass Sie auf der richtigen Seite sind.

4. Halten Sie Ihre Geräte mit der aktuellsten Software auf dem neuesten Stand.

SOFTWARE-UPDATES UND VERTEILUNG

Wenn man Software - sowohl Anwendungen als auch Betriebssysteme - auf dem neuesten Stand hält, kann man die Wahrscheinlichkeit verringern, dass eine Schwachstelle in der Software ausgenutzt wird. Cyberkriminelle können Malware entwickeln, die auf Schwachstellen in häufig genutzter Software abzielt, um ihre Rechte zu erweitern und/oder zusätzliche Malware zu verbreiten.

Da Online-Downloads - ob aus vertrauenswürdigen Quellen oder nicht - Malware enthalten können, kann die Einschränkung von Software-Downloads helfen, Probleme zu vermeiden. Je nachdem, wie Ihre Geräte verwaltet werden, gibt es mehrere Möglichkeiten, von der IT-Abteilung zugelassene Apps für Benutzer*innen bereitzustellen:

- Jamf Self Service Portal
- App Store
- Apple School Manager
- **Über Ihre MDM Plattform**

MULTI-FAKTOR-AUTHENTIFIZIERUNG

Die Multi-Faktor-Authentifizierung (MFA) ist eine erste Verteidigungslinie, um zu verhindern, dass kompromittierte Anmeldedaten zu einem Desaster führen. MFA erfordert zwei oder mehr Authentifizierungsfaktoren für die Anmeldung bei einem Konto. Zu diesen Faktoren gehören:

- Etwas, das Sie **kennen**, wie ein Passwort oder eine PIN
- Etwas, das Sie **haben**, wie eine Authentifizierungs-App oder einen Hardware-Anhänger
- Etwas, das Sie **sind**, wie ein Fingerabdruck, ein Netzhaut- oder Gesichtsscan

Geräte, die eine biometrische Authentifizierung bieten, wie z. B. ein iPad, können es jüngeren Schüler*innen erleichtern, die keinen Zugang zu einem weiteren Authentifizierungsgerät haben. Schulen oder Bezirke können eine weitere Verteidigungslinie hinzufügen, indem sie Single Sign-On mit MFA verwenden, um die Anzahl der Passwörter, die sich die Schüler merken müssen, zu begrenzen.

BACKUPS

Wie in früheren Abschnitten angedeutet, können Backups den ausschlaggebenden Unterschied ausmachen, ob Ihre Daten nach einem Ransomware-Angriff wiederhergestellt werden können oder nicht. Regelmäßige Backups können auch als Basis zur Wiederherstellung der Daten dienen, wenn Ihre Systeme durch andere Arten von Malware kompromittiert wurden. Allein diese beiden Vorteile machen Backups zu einem entscheidenden Faktor für die Erhaltung der Integrität und Sicherheit Ihrer Daten.

Besprechen Sie das Thema Sicherheit mit der Klasse

Idee für den Unterricht:

1. Lassen Sie die Schüler*innen eine Präsentation über einen Tipp zur Prävention erstellen und warum er zur Sicherheit aller beiträgt

GERÄTEVERWALTUNG

Die Verwaltung mobiler Geräte (Mobile Device Management, MDM) ist die Grundlage dafür, dass die Geräte in einem guten Zustand bleiben. MDM bietet Administrator*innen verschiedene Vorteile:

- Bestandsliste der mit den Schulressourcen verbundenen Geräte
- Bestimmung und Umsetzung der Sicherheitskonformität eines Geräts
- Aktualisierung der Geräte und ihrer Software auf die neuesten Versionen
- Einhaltung bestimmter Sicherheitsmaßnahmen, um das Risiko einer Datenverletzung zu verringern
- Beschränkung des Zugangs zu bestimmten Anwendungen und/oder Websites

CONTENT FILTER

Trotz guter Benutzerschulung passieren immer wieder Fehler, insbesondere auf mobilen Geräten, wo es schwierig ist, Links zu sehen oder eine Vorschau anzuzeigen. **Tools für den Content Filter** können dazu beitragen, Angriffe zu verhindern, indem sie bösartige Links blockieren. Wenn ein Schüler beispielsweise eine gut getarnte Phishing-E-Mail erhält und auf einen Link klickt, der darauf abzielt, seine Anmeldedaten abzugreifen, kann der Content Filter den Zugriff auf diese Website blockieren.

SICHERHEITS-FRAMEWORKS

Zwar verfügen nicht alle Schulen oder Bezirke über das Personal, die Finanzen oder die Ressourcen, um die Teile eines Sicherheits-Frameworks zu implementieren und durchzusetzen, macht es dennoch Sinn, darüber nachzudenken. Frameworks wie diese können IT-Abteilungen dabei helfen, die sicherste Konfiguration für ihre Ressourcen und Mitarbeiter*innen zu finden:

- **US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) Cyber Essentials**
- **UK Cyber Essentials**
- **Die IT Infrastructure Library (ITIL)**

jamf

Besprechen Sie das Thema Sicherheit mit der Klasse

Benutzerschulung:

Es ist nie zu früh, um mit der Aufklärung über Cybersicherheit zu beginnen. Studierende, Lehrkräfte und Mitarbeitende sollten über risikoreiche Verhaltensweisen informiert werden, z. B:

- Anklicken von Links, ohne deren Legitimität zu prüfen
- Weitergabe von Anmeldedaten
- Anschließen unbekannter USB-Laufwerke oder anderer Wechselmedien an ihr Gerät
- Herunterladen von Software von Websites Dritter
- Keine Aktualisierungen ihre Geräte oder Anwendungen

Phishing-Angriffe sind weit verbreitet und Benutzer*innen sollten wissen, wie sie Phishing-Versuche erkennen. Dinge wie diese können Indikatoren sein:

- Ähnlich aussehende URLs mit Sonderzeichen oder seltsamer Formatierung
- Rechtschreibfehler oder ungewöhnliche Sprache in E-Mails (obwohl die Angreifer immer bessere Nachrichten erstellen)
- Aufruf zum dringenden Handlungsbedarf
- Ungewöhnliche und/oder unaufgeforderte Nachrichten, auch von Personen, die Sie kennen

IMPLEMENTIERUNG: JAMF SCHOOL UND JAMF SAFE INTERNET

Wir haben über einige Möglichkeiten zur Prävention von Malware gesprochen. Aber wie setzen wir diese Strategien tatsächlich um?

Jamf School

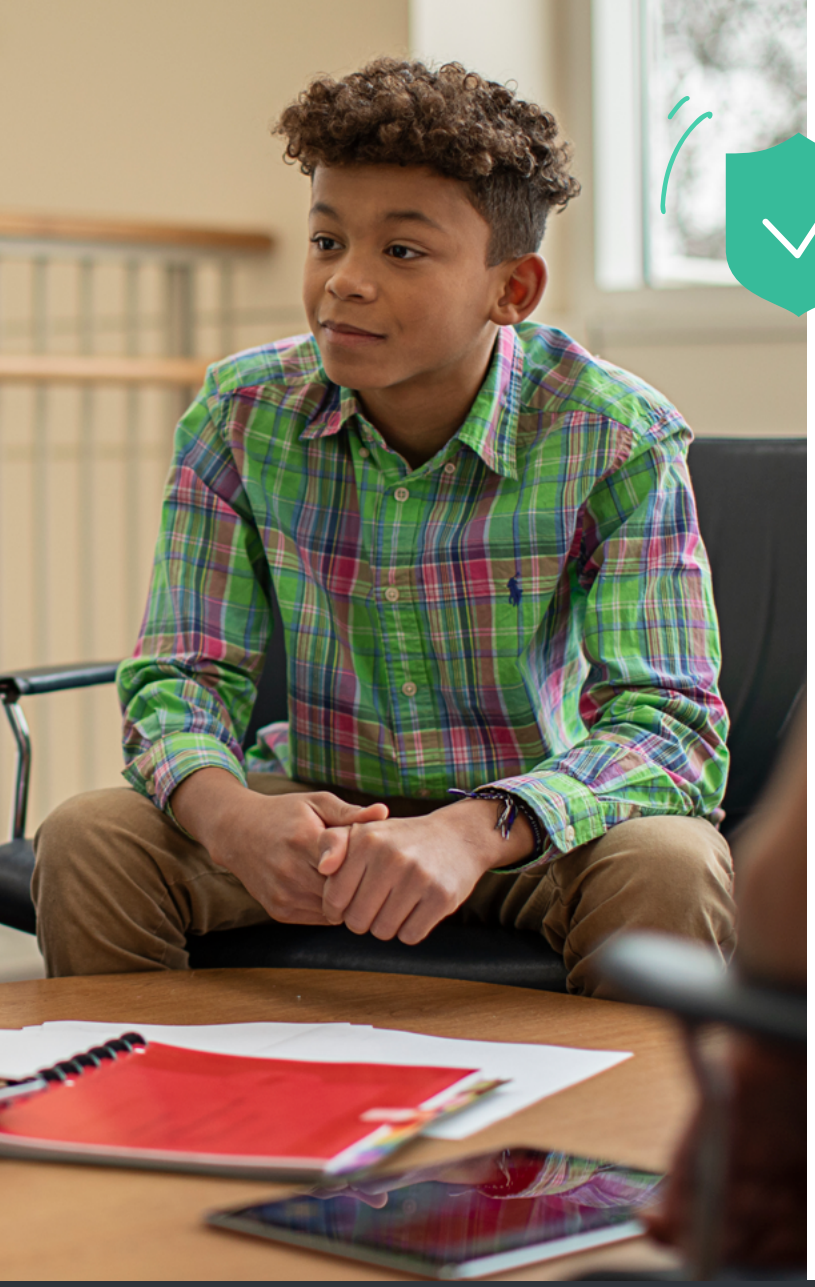
Wir haben bereits erwähnt, dass MDM die Grundlage für die Sicherheit Ihrer Geräte darstellt. Das allein reicht zwar nicht aus, ist aber von entscheidender Bedeutung, da es die nötige Transparenz über die Geräte schafft, die mit den Daten von Schüler*innen und Mitarbeiter*innen interagieren.

In gewisser Weise **bietet die Verwaltung mehr Sicherheit.**

Jamf School ist ein bildungsorientiertes MDM für Schulen, das die Bereitstellung, Verwaltung und Sicherung von Mac, iPad, iPhone und Apple TV vereinfacht. Das Angebot:

- Transparenz über verwaltete Geräte, Benutzer*innen und Apps
- Einfache Bereitstellung von Software und Upgrades
- Die Möglichkeit, die Sicherheitseinstellungen des Geräts zu konfigurieren, einschließlich Passcode-Richtlinien und Inhaltsfilterung
- Solide und sichere App-Bereitstellung und -Aktualisierung mit überprüften Apps
- Tools für das Unterrichtsmanagement, um die Konzentration der Lernenden aufrechtzuerhalten

Sicherheit fängt bei der Verwaltung an: Wenn Sie Ihre Geräte kennen - und wissen, was sich darauf befindet -, können Sie die Sicherheit des Geräts unterstützen: von der Aktualisierung der erforderlichen Software bis hin zur Einrichtung spezieller Sicherheitskontrollen.



Jamf Safe Internet

Jamf Safe Internet geht über MDM hinaus und schafft eine sichere Lernumgebung, indem es den Schüler*innen ermöglicht, privat zu surfen, ohne auf Malware oder andere gefährliche Inhalte zu stoßen. Jamf Safe Internet ist mit Geräten von Apple, ChromeOS und Windows kompatibel und bietet folgende Funktionen:

Vollständig anpassbar mit der Flexibilität, Richtlinien, die für verschiedene Gruppen gelten, basierend auf Gerätetyp, Geografie oder anderen Attributen, einfach festzulegen oder zu ändern. Jamf Safe Internet funktioniert mit jedem verwalteten Gerät, unabhängig davon, ob es sich in einem Warenkorb befindet, von der Schule zugewiesen wurde oder in persönlichem Besitz ist.

Leistungsstarker Content Filter mit:

- Durchsetzung von Google Safe Search
- Eingeschränkter Modus für YouTube, um ausschließlich Bildungsinhalte anzuzeigen
- Fortschrittliches maschinelles Lernen zur Erkennung und Verhinderung unentdeckter Bedrohungen
- Netzwerkinterner Echtzeitschutz zur Verhinderung des Zugriffs auf Phishing-Seiten und andere bösartige Domains

Sicherheit ohne Überwachung, indem den Schüler*innen die Freiheit gegeben wird, das Internet zu erkunden und ein digitales Bewusstsein zu entwickeln, ohne ihre Privatsphäre zu verletzen oder sie in Gefahr zu bringen.

jamf

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

Los geht's

www.jamf.com/de/