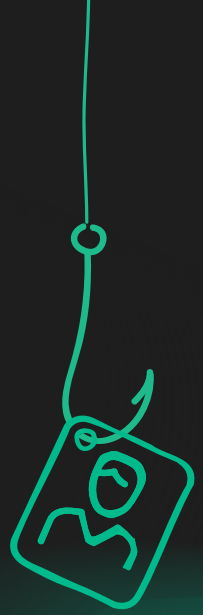
Social Engineering an Schulen

für Einsteiger

jamf

Kinder sind in der Schule, um zu lernen - aber nicht nur, um zu lernen. Die Schule hilft ihnen dabei, sich in einem sozialen Umfeld zurechtzufinden, ein gesundes Selbstwertgefühl zu entwickeln und Bestätigung durch Gleichaltrige oder andere Personen zu erfahren. Es ist eine turbulente Zeit, die nicht immer von gutem Urteilsvermögen geprägt ist.



Angreifer wissen das; und genau deshalb nehmen Sie Schulen mit Social-Engineering-Angriffen ins Visier.

Sie bauen Druck auf und hoffen auf die Naivität der Schüler, damit sie die Tür öffnen.

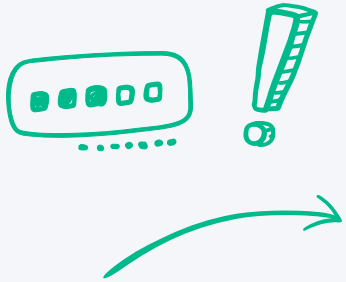
In diesem E-Book geht es um folgende Themen:

- **Was ist Social Engineering?**
- **Typische Taktiken**
- **Wie es sich in Schulen manifestiert**
- **Die Tools und Techniken zur Verhinderung von Angriffen**

Was ist Social Engineering?

Beim Social Engineering werden psychologische Methoden eingesetzt, um Benutzer zur Preisgabe vertraulicher Informationen zu verleiten. Es kann als eigenständige Methode eingesetzt werden, etwa in Form einer Website, die wie eine vertraute Anmeldeseite aussieht, aber stattdessen Zugangsdaten stiehlt. Oder es kann in Verbindung mit anderen Vektoren verwendet werden, indem es zum Beispiel Malware verbreitet.

Social Engineering zielt direkt auf den Faktor Mensch innerhalb Ihrer Sicherheitsstrategie ab. Dies ist eine äußerst verbreitete Methode, die laut dem **2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience** **andere Angriffsvektoren um mindestens 45 % übertrifft.**



Warum muss die IT nach Social Engineering suchen?

Weil es Ihre Schule anfällig für Angriffe macht.
Stellen Sie sich folgende Situation vor:

Angreifer können Ihre Kontrollmechanismen umgehen:

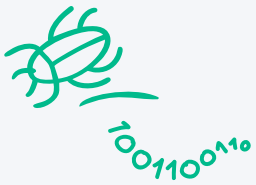
Wenn Ihre IT-Konfigurationen und Sicherheitsvorkehrungen nicht auf Social Engineering ausgerichtet sind, können sie umgangen werden - denn wenn der Angreifer über Anmeldedaten verfügt, kann sein Anmeldeversuch ohne geeignete Tools legitim erscheinen.

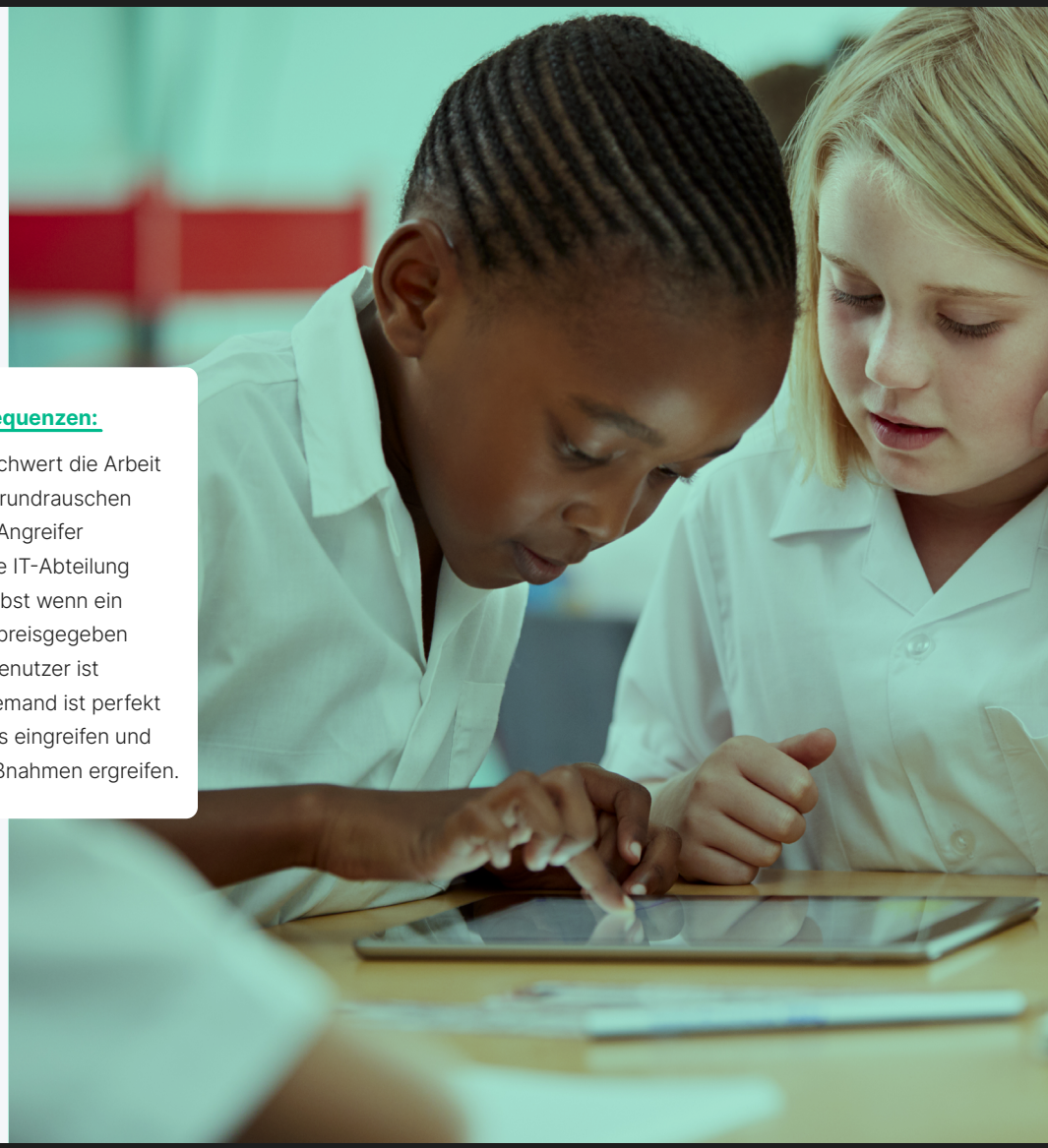
Seitwärtsbewegung ist ein Risiko:

Ein einziges kompromittiertes Konto kann Tür und Tor zu Ihren Systemen öffnen und das Schadensausmaß vergrößern, da Angreifer von dort aus in sensiblere Bereiche vordringen können.

Die IT trägt die Konsequenzen:

Social Engineering erschwert die Arbeit der IT, indem es das Grundrauschen erhöht. Und wenn ein Angreifer erfolgreich ist, trägt die IT-Abteilung die Verantwortung, selbst wenn ein Benutzer seine Daten preisgegeben hat. Die Vorsicht der Benutzer ist entscheidend, aber niemand ist perfekt – die IT-Abteilung muss eingreifen und zusätzliche Schutzmaßnahmen ergreifen.





Häufige Social-Engineering-Taktiken

Phishing

Phishing ist eine gängige Form des Social Engineerings. Die Angreifer könnten sich als Schulpersonal oder Dienstleister ausgeben, legitime Websites nachahmen und ein Gefühl der Dringlichkeit erzeugen, um Benutzer dazu zu bringen, ihre Daten preiszugeben.

Malvertising

Bösartige Werbung oder Malvertising nutzt Online-Anzeigen, um Benutzer zum Herunterladen von Malware zu verleiten oder ihre Anmeldedaten zu stehlen.

Pretexting

Pretexting kann sehr unterschiedlich aussehen, dient aber in der Regel dazu, das Vertrauen des Benutzers zu gewinnen. Angreifer können sich als Autoritätsperson oder Gleichgesinnter ausgeben, damit die Benutzer ihnen vertrauen, um ihre Informationen preiszugeben.

Baiting

Baiting (engl. für „Ködern“) locken die Benutzer mit unwiderstehlichen Angeboten: kostenloses Geld, Anerkennung, exklusive Inhalte und mehr. Doch wenn der Benutzer auf den Link klickt, installiert er Malware oder wird auf Phishing-Seiten weitergeleitet.

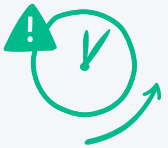
SEO-Poisoning

Angreifer schalten Anzeigen in Suchmaschinen, um ihre bösartigen Fake-Seiten ganz oben in den Suchergebnissen zu platzieren, damit ahnungslose Benutzer darauf klicken.

Prompt Bombing

Angreifer senden wiederholt Anfragen zur Multi-Faktor-Authentifizierung, um den Benutzer so lange zu nerven, bis er ihnen Zugriff gewährt.

Diese Techniken gibt es schon seit einiger Zeit. Neu sind jedoch die Methoden mit KI. Dadurch wurden die Karten ganz neu gemischt. In seinem **Bericht „Cost of a Data Breach Report 2025**“ stellte IBM fest, dass einer von sechs Datenverletzungen auf KI-gesteuerte Angriffe zurückzuführen ist.



Mit **generativer KI** können Angreifer ***„die Zeit, die für die Erstellung einer überzeugenden Phishing-E-Mail benötigt wird, von 16 Stunden auf nur 5 Minuten reduzieren“.***

KI führt zu schnelleren und überzeugenderen Phishing-Angriffen und Deepfakes. Die Schulen müssen auf diese technologischen Fortschritte reagieren, insbesondere angesichts der hohen Anfälligkeit ihrer jungen Benutzer.

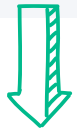
Wie sich Social Engineering in Schulen manifestiert

Social Engineering taucht bei allen Arten von Cyberangriffen auf. Der **Verizon 2025 Data Breach Investigations Report** stellte fest, dass bei **17 % der Angriffe auf den Bildungssektor** Social-Engineering-Techniken zum Einsatz kamen.

Wie dies konkret aussieht, kann variieren, da Social Engineering viele Formen annimmt und sich ständig weiterentwickelt. Hier sind einige mögliche Szenarien:

Online-Spiele? Sie wurden gerade hereingelegt.

Ein Schüler der Mittelstufe sucht im Internet nach Spielen, nachdem er seine Schularbeiten erledigt hat. Sie landen auf einer Website, auf der mit Gratisgeld für ihr Lieblings-Online-Spiel geworben wird! Sie können nicht widerstehen und klicken auf den Link, der sie zu einer Website führt, die ihre Zugangsdaten stiehlt und ihnen virtuellen Reichtum verspricht – im Gegenzug für ihre Anmeldedaten.



Manchmal sollte man diesem geschenkten Gaul lieber ins Maul schauen

Die neue Lehrkraft ist bestrebt, den Administratoren der Schule zu gefallen. So sehr, dass sie nicht einmal zögern, wenn ihr „Schulleiter“ eine E-Mail schickt und nach Gutscheincodes fragt. Diese Lehrkraft ist zu neu, um zu erkennen, dass ihr Schulleiter nicht ***ganz*** so redet wie der Inhalt der E-Mail.

Richtig oder falsch: Dieser Download ist sicher

(Spoiler: falsch)

Ein Gymnasiast bereitet sich auf die Aufnahmeprüfungen für die Uni vor. Sie suchen nach Ressourcen zur Testvorbereitung. Das Suchergebnis oben auf der Seite ist ein gesponserter Link, der für kostenlose Übungstests wirbt. Der Schüler muss lediglich die Software zur Prüfungsvorbereitung herunterladen, die – Überraschung – Malware enthält.

Sie werden richtig bekannt … wenn Ihre Daten online offengelegt werden.

Eine Gruppe von Grundschülern erhält eine E-Mail zu einem Beliebtheitswettbewerb an der Schule – stimme für den beliebtesten Schüler ab und schau, ob du gewinnst! Wir müssen nur überprüfen, ob du wirklich Schüler an deiner Schule bist; kannst du uns einige personenbezogen Daten geben?

Social Engineering im Keim ersticken

Was können Sie tun, um zu verhindern, dass Social Engineering Ihre Benutzer ausnutzt und Ihre Datensicherheit bedroht? Dabei müssen Sie zwei Aspekte berücksichtigen: **Ihre Benutzer und Ihre Technik.**

Benutzerschulung

Ihre Benutzer, insbesondere die jüngeren, kennen noch nicht alle guten und schlechten Seiten des Internets. Viele hinterfragen noch nicht, was sie online sehen. Im Idealfall ist die Vermittlung von digitaler Souveränität und Verantwortung fest im Lehrplan Ihrer Schule verankert. Die digitale Souveränität lehrt die Schüler, das Internet verantwortungsvoll und sicher zu nutzen.

Dazu gehören:

- **Altersgerechte Erklärungen** zu gängigen Cyber-Bedrohungen
- **Beispiele** für verdächtige Websites/Inhalte
- Förderung von ethischem und verantwortungsvollem **Verhalten** im Internet

Und natürlich brauchen auch Ihre Lehrkräfte/Mitarbeiter Schulungen. Sie sollten Folgendes schulen:

- **Phishing-E-Mail-Simulationen**
- Regelmäßige, vorgeschriebene **Schulungen** zur Konformität
- Förderung einer **Kultur der Transparenz** – Benutzer sollten umgehend mit der IT-Abteilung sprechen, wenn sie befürchten, dass sie auf einen Social-Engineering-Angriff hereingefallen sind

Technische Hilfsmittel und Richtlinien als weitere Verteidigungslinie

Angreifer haben es nicht ohne Grund auf den Faktor Mensch abgesehen: Es erfordert weniger technischen Aufwand und verspricht eine höhere Erfolgswahrscheinlichkeit. Und weil wir Menschen alle fehlbar sind, brauchen wir eine weitere Schutzebene.

Inhaltsfilterung

Die Inhaltsfilterung blockiert bösartige Inhalte, selbst wenn ein Benutzer auf einen bösartigen Link klickt. Inhaltsfilterung lässt sich über Erlaubnis- und Blocklisten realisieren, die explizit festlegen, welche Websites erlaubt sind – und welche nicht. Dies hat jedoch Grenzen. Es ist schlicht unmöglich, jede nützliche Website explizit freizugeben oder jede potenziell schädliche Seite vorab zu blockieren. Außerdem ist dies nicht das Internet, das die Schüler nach ihrem Abschluss sehen werden.

Effektiver ist eine Filterung, die breite Kategorien blockiert. Dadurch müssen die IT-Administratoren keine Domains explizit auflisten. Stattdessen kategorisiert es jede Website und entscheidet anhand ihrer Kategorie, ob sie blockiert werden soll. Websites für Erwachsene, Glücksspiel-Websites, Dateifreigaben, Netzwerke, gewalttätige oder anstößige Websites und vieles mehr - sie alle werden auf der Grundlage Ihrer Konfigurationen blockiert. Wenn Sie KI und maschinelles Lernen für intelligente Filterung hinzufügen, haben Sie noch mehr Vorteile.

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) bietet eine zusätzliche Sicherheitsebene bei der Anmeldung. Wenn die Anmeldedaten eines Benutzers kompromittiert ***werden***, verringert MFA die Wahrscheinlichkeit, dass ein Angreifer tatsächlich auf den Account zugreifen kann. MFA erfordert mindestens zwei dieser Authentifizierungsmethoden:

- **Etwas, das Sie kennen,** wie ein Passwort, eine PIN oder eine Sicherheitsfrage
- **Etwas, das Sie sind,** wie Ihr Fingerabdruck oder Ihr Gesicht
- **Etwas, das Sie haben,** wie ein anderes Gerät oder einen Sicherheitsschlüssel

Technische Hilfsmittel und Richtlinien als weitere Verteidigungslinie

Single Sign-On

Wenn Sie einen Identitätsdienst (IdP) zu Ihrem Tech-Stack hinzufügen, können Sie echtes Single Sign-On (SSO) etablieren, das Ihrem IdP signalisiert, ***alle*** Konten eines Benutzers freizuschalten. Das bedeutet, dass sich die Benutzer weniger Passwörter merken müssen und somit auch weniger Möglichkeiten zur Kompromittierung haben. Aber bedeutet das nicht, dass Angreifer nur ein Passwort brauchen, um sich überall anzumelden?

Zum Glück nicht, denn SSO nutzt in der Regel die MFA. Sie können es so einrichten, dass ein biometrisches Merkmal wie der Fingerabdruck eines Schülers oder einer Schülerin erforderlich ist. SSO reduziert nicht nur die Passwortmüdigkeit und die Anzahl potenzieller Einfallstore, sondern trägt auch aktiv dazu bei, den Diebstahl von Zugangsdaten zu verhindern. Angenommen, ein Benutzer landet auf einer Fake-Website: Da Ihr IdP den Domänennamen nicht erkennt, verweigert er die Anmeldung – so wird verhindert, dass der Benutzer seine Zugangsdaten preisgibt.

Geräteverwaltung

Die bereits erwähnten Tools sind großartig. Aber ohne ein Mobile Device Management (MDM) sind sie jedoch nur schwer zu implementieren. Mit MDM haben IT-Administratoren mehrere Vorteile:

- Transparente Sicherheitslage der Geräte
- Festlegung von Sicherheitsrichtlinien und sicheren Konfigurationen
- Konfiguration von Geräteeinstellungen und -beschränkungen, wie beispielsweise einen obligatorischen Passcode oder der Zugriff auf bestimmte Apps
- Geräte mit der neuesten Software aktuell halten
- Bereitstellung von Lösungen zur Inhaltsfilterung

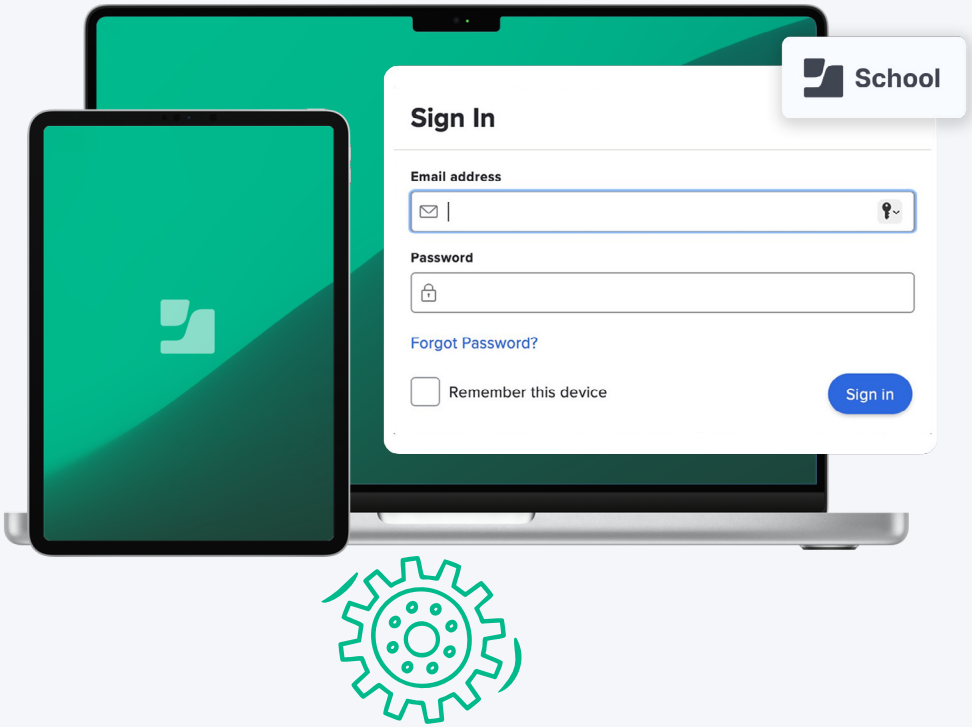
Implementierung: Jamf School und Jamf Safe Internet

Jamf School

Jamf School ist ein MDM, das speziell für Schulen entwickelt wurde.
Es enthält folgende Funktionen:

- **Vorgefertigte Gerätekonfigurationen**, die die deklarative Geräteverwaltung nutzen
- **Gerätebestand**, damit die Admins wissen, welche Geräte auf die Schulressourcen zugreifen
- **Transparenz** über den Gerätestatus, damit eventuelle Probleme schnell behoben werden können
- Die Möglichkeit, **Einschränkungen** und **Einstellungen** für ein Gerät festzulegen, einschließlich eines erforderlichen Passcodes
- **Kompatibilität mit SSO** (mit zusätzlichem Identitätsdienst)
- **Eine einfache Möglichkeit** für Lehrkräfte, die IT-Genehmigung für Apps anzufordern
- Und noch viel **mehr**!

Jamf School bietet Ihrer Schule die Basis für sichere Geräte, die so eingerichtet werden können, dass sie Social-Engineering-Angriffen standhalten.

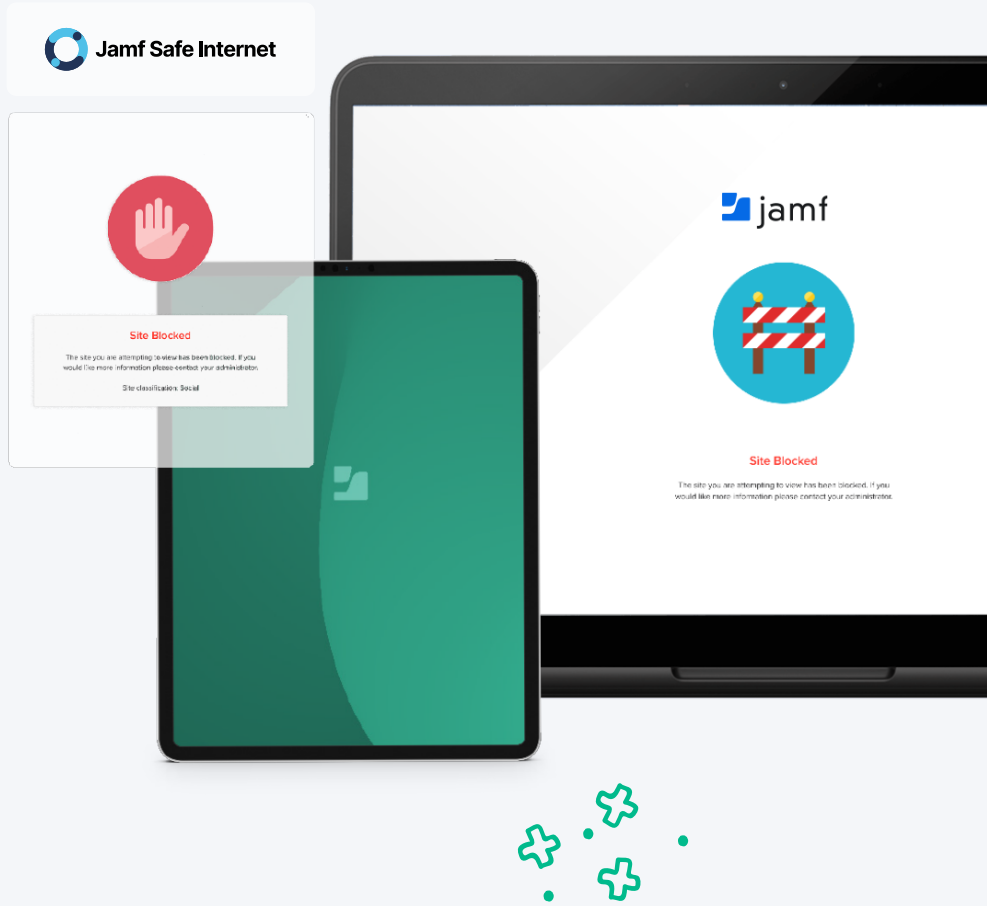


Jamf Safe Internet

Jamf Safe Internet geht in Sachen Sicherheit noch einen Schritt weiter und ist mit Apple-, Chromebook- und Windows-Geräten kompatibel. Jamf Safe Internet ist vollständig anpassbar, sodass Sie ganz einfach Richtlinien für verschiedene Gerätegruppen auf der Grundlage ihres Standorts, ihres Typs oder anderer Attribute festlegen oder ändern können. Es funktioniert mit Geräten, unabhängig davon, ob sie sich im Warenkorb befinden, von der Schule zugewiesen werden oder ob es sich um ein eigenes Gerät des Schülers handelt.

Zur Abwehr von Bedrohungen wie Social Engineering **bietet Jamf Safe Internet**:

- **Leistungsstarke Inhaltsfilterung**, unterstützt durch KI und ML: blockiert den Zugriff auf Phishing-Websites, noch bevor diese als bösartig erkannt werden
- **Blockierung von DNS**- und **Domainnamen** zum Schutz vor DNS-Spoofing
- **Geräteseitige Inhaltsfilterung** auf dem iPad für umfassenden Schutz
- **Netzwerkinterner Schutz** vor bösartigen Websites, bevor sie Geräte infizieren können
- **Google SafeSearch** und **Google Safe Browsing** verpflichtend, um zu verhindern, dass bösartige oder ungeeignete Websites in der Suche angezeigt werden



Die gesamte Sicherheit ohne Überwachung: Die Schüler können frei im Internet surfen und ihre Fähigkeiten als digitale Bürgerinnen und Bürger entwickeln, ohne dass ihre Privatsphäre verletzt wird. Mit sicherer Technologie im Klassenzimmer gewinnen alle:

Die Lehrkräfte
können sich auf das Lernen konzentrieren, ohne dass es zu Login-Problemen und Unterbrechungen kommt.

Die Schüler erhalten
die Freiheit, neue Dinge auszuprobieren und zu lernen - und das auf sichere Weise.

IT-Admins
können sich auf andere Aufgaben konzentrieren, da sie wissen, dass ihre Daten zuverlässig geschützt sind.

Möchten Sie erleben, wie Ihre Schule durch Technologie gestärkt werden kann?

Probieren Sie Jamf aus