KEEPER®

Cybersicherheit in Schulen 2025

Ein Leitfaden für Familien und Lehrkräfte für sichereres digitales Lernen

Kostenlose Ressource von Keeper Security | Verfügbar auf flexyourcyber.com

Überblick

Klassenzimmer sind vernetzter denn je – und damit auch die Bedrohungen, die gegen sie gerichtet sind. Ransomware-Angriffe beeinträchtigen Gemeinden, KI-generierte Betrügereien zielen auf Schüler ab und Phishing-Kampagnen sind immer schwerer zu erkennen. Mit digitalen Plattformen, die heute für Hausaufgaben, die Zusammenarbeit im Klassenzimmer und die Verwaltungsabläufe von zentraler Bedeutung sind, ist Cybersicherheit zu einer grundlegenden Anforderung des Bildungswesens geworden und nicht mehr zu einer Option.

Dieser Leitfaden bietet Administratoren, Lehrkräften, Eltern und Schülern Experteneinblicke und umsetzbare Schritte zur Stärkung der digitalen Sicherheit. Durch die Kombination von Bewusstsein, Best Practices und offener Kommunikation können Schulen und Familien sichere Lernumgebungen schaffen, die sowohl die akademische Kontinuität als auch persönliche Daten schützen.

Die Bedrohungslandschaft in 2025

Cyberangriffe auf das Bildungswesen nehmen zu – und die Auswirkungen sind härter denn je.

- **Ransomware nimmt zu:** In der ersten Hälfte des Jahres 2025 stiegen die Angriffe auf Schulen, Hochschulen und Universitäten im Vergleich zum Vorjahr um 23 % (Comparitech)
- **Schulen sind die Hauptziele:** 82 % der K-12-Schulen in den USA erlebten zwischen Juli 2023 und Dezember 2024 mindestens einen Cybervorfall (Center for Internet Security)
- **Finanzieller Druck wächst:** Durchschnittliche Lösegeldforderungen erreichen mittlerweile 556.000 US-Dollar (Comparitech)
- **Phishing ist schwerer zu erkennen:** KI-gestützte bösartige E-Mails haben sich in den letzten zwei Jahren verdoppelt (Verizon DBIR)

Das Fazit: Das Bildungswesen ist heute eine der am meisten ins Visier genommenen Bereiche, und Angreifer nutzen KI, um ihre Taktiken überzeugender denn je zu machen.

Top 5 der digitalen Risiken, mit denen Schüler und Schulen konfrontiert sind

Schwache und wiederverwendete Anmeldeinformationen

Recycelte oder vorhersehbare Passwörter sind nach wie vor der einfachste Einstiegspunkt für Angreifer

Verwenden Sie einen Passwortmanager, um starke, eindeutige Anmeldedaten zu generieren und zu speichern

Gemeinsame Konten und schlechte Privilegienkontrolle

Ein einziger kompromittierter geteilter Login kann ganze Klassenzimmer, Abteilungen oder sogar Gemeinden Angriffen aussetzen

Eliminieren Sie gemeinsam genutzte Konten und erzwingen Sie den Zugriff mit den geringsten Rechten

Phishing und Social-Media-Betrug

Cyberkriminelle nutzen Vertrauen aus, indem sie sich als Mitarbeiter, Klassenkameraden oder Familienmitglieder ausgeben

Überprüfen Sie Identitäten über vertrauenswürdige Kanäle, bevor Sie Informationen weitergeben

Ungesichertes WLAN zu Hause oder in der Öffentlichkeit

Offene oder schlecht geschützte Netzwerke ermöglichen es Angreifern, sensible Daten abzufangen

Verwenden Sie ein passwortgeschütztes WLAN oder ein VPN auf Schulgeräten

KI-gestützt Falschinformationen und Deepfakes

Gefälschte Audio- und Videoinhalte können Schüler und Mitarbeiter dazu verleiten, vertrauliche Informationen weiterzugeben oder schädliche Maßnahmen zu ergreifen

Schulen Sie die Nutzer darin, Warnsignale zu erkennen, und ermutigen Sie sie, Verdachtsfälle zu melden

Das Cybersecurity-Playbook: Strategien und Tools

Für Schulen

- [ ] Setzen Sie starke Passwortrichtlinien und Multi-Faktor-Authentifizierung (MFA) durch
- [ ] Implementieren Sie Privileged Access Management (PAM) zur Sicherung kritischer Systeme
- [ ] Bieten Sie kontinuierliche Cybersicherheitsschulungen für alle Mitarbeiter
- [ ] Führen Sie regelmäßige Schwachstellenbewertungen durch und pflegen Sie einen klaren Plan zur Reaktion auf Vorfälle
- [ ] Sichern Sie regelmäßig kritische Daten und testen Sie Wiederherstellungsprozesse
- [ ] Prüfen Sie Drittanbieter und Partner auf Compliance- und Sicherheitspraktiken

Für Eltern

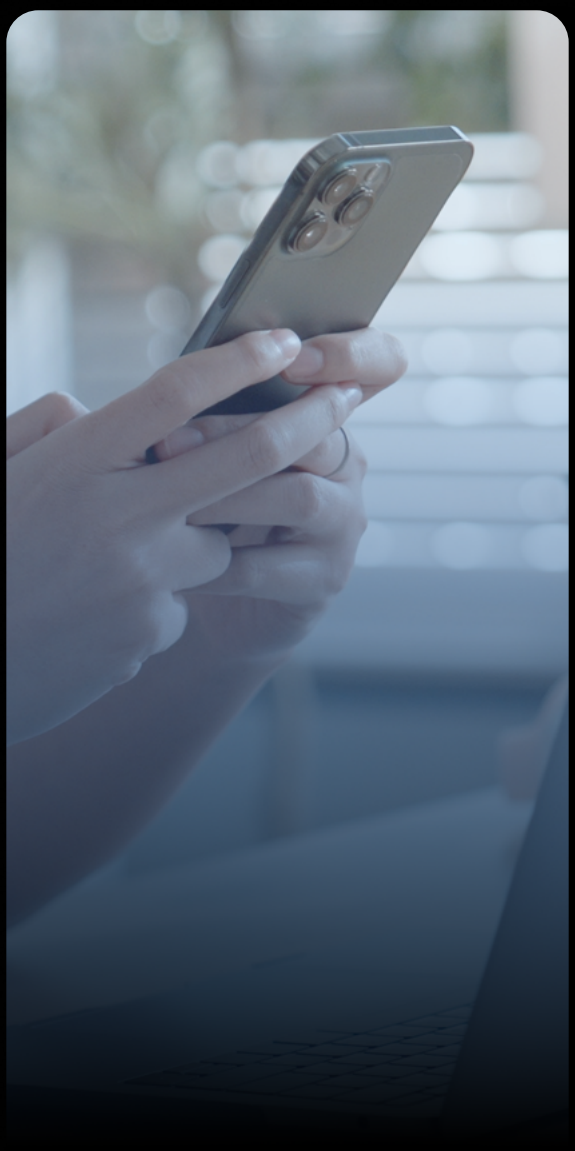
- [ ] Sichern Sie Heimgeräte mit starken, eindeutigen Passwörtern
- [ ] Aktivieren Sie automatische Softwareupdates
- [ ] Überwachen Sie die Online-Aktivitäten und fördern Sie verantwortungsbewusste Surfgewohnheiten
- [ ] Verwenden Sie die Kindersicherung, um riskante Inhalte und Downloads einzuschränken
- [ ] Etablieren Sie ein sicheres digitales Verhalten durch eine gute Passwort-Hygiene

Für Schüler/Studierende

- [ ] Halten Sie Passwörter privat, auch vor Freunden
- [ ] Vermeiden Sie es, auf unbekannte Links zu klicken oder nicht verifizierte Dateien herunterzuladen
- [ ] Seien Sie vorsichtig, wenn Sie persönliche Daten online weitergeben
- [ ] Sprechen Sie darüber, wenn sich etwas online verdächtig oder unangenehm anfühlt
- [ ] Ignorieren Sie nicht Erinnerungen an das Aktualisieren von Software und Geräten

Starter für ein Eltern-Kind-Cybergespräch

- [ ] ,,Was würdest du tun, wenn jemand nach deinem Passwort fragen würde?“
- [ ] ,,Woran erkennst du, ob eine Nachricht oder ein Video echt ist?“
- [ ] ,,Warum solltest du unterschiedliche Passwörter für verschiedene Konten verwenden?“
- [ ] ,,Was würdest du tun, wenn du online etwas siehst, das dir unangenehm ist?“
- [ ] ,,Warum ist es wichtig, vor dem Herunterladen einer neuen App oder eines neuen Spiels nachzufragen?“



Der KI-Faktor
Betrug ist die neue Normalität

KI-Tools ermöglichen es Cyberkriminellen, Angriffe mit alarmierender Realitätsnähe zu skalieren. Das Klonen von Stimmen und Deepfakes können vertrauenswürdige Personen imitieren. KI-gestützte Phishing-E-Mails sind überzeugender und schwerer zu erkennen.

Warnsignale für KI-Betrug

- Nachrichten, die zum sofortigen Handeln auffordern
- Anfragen nach Geld, Geschenkkarten oder persönlichen Informationen
- Seltsame Phrasierungen, unpassende Töne oder ungewöhnliche Bilder
- Ein allgemeines Gefühl, dass ‚etwas nicht stimmt“

So reduzieren Sie das Risiko

- Verwenden Sie in der Familie ein geheimes Wort oder eine geheime Phrase, um Identitäten zu bestätigen
- Beenden Sie verdächtige Anrufe und stellen Sie die Verbindung über offizielle Nummern wieder her
- Beschränken Sie das öffentliche Posten von Videos und Sprachaufzeichnungen

Gemeinsam Cybervertrauen aufbauen

Digitales Lernen ist nicht mehr wegzudenken, und damit bleiben auch die Risiken. Aber mit Bewusstsein, Vorbereitung und den richtigen Tools können Schulen und Familien den Cyberkriminellen immer einen Schritt voraus sein. Das Praktizieren sicherer Gewohnheiten, die Aufrechterhaltung einer offenen Kommunikation und die Wachsamkeit sind der Schlüssel zur Schaffung sichererer Klassenzimmer und Haushalte.

Cybersicherheit ist nicht nur die Aufgabe der IT, sondern liegt in der Verantwortung aller.

Wichtige Erkenntnisse

- **Bildung ist heute ein Top-Ziel für Cyberangriffe**
  Angreifer wissen, dass Schulen oft begrenzte Budgets und IT-Personal besitzen, aber dennoch über wertvolle sensible Daten verfügen
- **Cybersicherheit geht über das Klassenzimmer hinaus**
  Eltern und Schüler spielen eine ebenso wichtige Rolle wie Administratoren bei der Reduzierung von Risiken durch sichere digitale Gewohnheiten
- **KI verändert das Spiel**
  Deepfakes und KI-gesteuertes Phishing werden bleiben – Verifizierung, Skepsis und Best Practices für Cybersicherheit sind für Familien und Schulen gleichermaßen unerlässlich
- **Resilienz hängt von Menschen ab, nicht von Technologie**
  Starke Abwehrmaßnahmen kombinieren technische Schutzmaßnahmen (MFA, PAM, sichere Netzwerke) mit Schulungen, Kommunikation und klaren Richtlinien
- **Cybervertrauen wird gemeinsam aufgebaut**
  Offene Gespräche zwischen Pädagogen, Eltern und Schülern stärken das Vertrauen und schaffen eine gemeinsame Sicherheitskultur

Weitere Ressourcen finden Sie unter flexyourcyber.com