KEEPER | Pressemitteilung

Keeper Security rät zu erhöhter Cybersicherheit für die Rückkehr der Schüler in den Unterricht

Eskalierende Cyberbedrohungen im Bildungswesen erfordern aktive Maßnahmen, einschließlich robuster Passwortverwaltung und Sensibilisierungstraining.

MÜNCHEN, 29. August 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang und Remote-Verbindungen, ruft Schüler, Eltern und Lehrer für das neue Schuljahr auf, angesichts der zunehmenden Cyberangriffe der digitalen Sicherheit eine hohe Priorität einzuräumen. Aufgrund der zunehmenden Abhängigkeit von Technologie im Bildungswesen – von Online-Lernplattformen bis hin zur digitalen Verwaltung – sind robuste Cybersicherheitsmaßnahmen wichtiger denn je.

Eskalierende Cyberbedrohungen im Bildungswesen

Der Verizon 2024 Data Breach Investigations Report bestätigt einen besorgniserregenden Trend: Der Bildungssektor war im Jahr 2023 mit 1.780 Cybervorfällen konfrontiert, von denen 1.537 zu einer Offenlegung von Daten führten. Der dramatische Anstieg der Vorfälle um 258 Prozent und der Anstieg der Datenschutzverletzungen um 545 Prozent im Vergleich zum Vorjahr verdeutlicht die Schwachstellen im Bildungssektor.

„Cybersicherheit ist nicht nur eine Aufgabe für Unternehmen. Sie ist auch ein elementarer Aspekt in der Bildung und damit für die Zukunft aller Schüler“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Da Schüler und Lehrer zunehmend von digitaler Technologie innerhalb und außerhalb des Klassenzimmers abhängig sind, ist es von größter Bedeutung, dass diese Umgebungen sicher bleiben.“

Aktive Schritte für digitale Sicherheit

Keeper empfiehlt vier grundlegende Maßnahmen für Schüler, Eltern und Lehrer, um die digitale Sicherheit zu erhöhen:

1. Passwort-Manager verwenden: Erstellen und Speichern von starken, eindeutigen Passwörtern für alle schulbezogenen Konten, um das Risiko eines unbefugten Zugriffs zu minimieren.
2. Regelmäßige Software-Updates: Alle Geräte und Anwendungen mit aktuellen Sicherheits-Patches auf dem neuesten Stand halten, um sich vor bekannten Sicherheitslücken zu schützen.
3. Umfassende Ausbildung und Schulung: Schüler und Mitarbeiter sollten darin geschult werden, Phishing und andere Social-Engineering-Betrügereien zu erkennen und verdächtige Aktivitäten sofort zu melden.
4. Sichere Netzwerke: Schulische und private Wi-Fi-Netzwerke sollte mit starken Passwörtern und Verschlüsselung gesichert werden, um unbefugte Zugriffe zu verhindern.

Verbesserung der Cybersicherheit mit einem Passwortmanager

Keeper bietet Tools zur Bekämpfung von Cyberbedrohungen und zur Verbesserung der digitalen Sicherheit. Mit dem Keeper Passwortmanager können Schüler, Eltern, Lehrer und

Administratoren starke, eindeutige Passwörter sowie Multi-Faktor-Authentifizierungscodes (MFA) für jedes Konto erstellen und sicher speichern. Die Plattform identifiziert schwache oder wiederverwendete Passwörter und erleichtert den sicheren Austausch von Passwörtern zwischen Lehrern und Schülern sowie zwischen Familienmitgliedern. Durch die Integration von Keeper in das tägliche digitale Leben können die Nutzer ihre Online-Sicherheit erheblich verbessern.

Eltern sollten zudem mit ihren Kindern über Cybersicherheit sprechen und aktive Maßnahmen ergreifen, einschließlich robuster Sicherheitssoftware und sicheren Passwörtern. Schulen sind aufgerufen, ihre Cybersicherheitsrichtlinien zu überprüfen und zu verstärken, wo immer dies möglich ist, und sicherzustellen, dass umfassende Schulungen verfügbar sind, um potenzielle Bedrohungen zu erkennen und darauf zu reagieren.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf KeeperSecurity.com.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de