KEEPER | Pressemitteilung

Bleiben Sie sicher an diesem Amazon Prime Day: Expertentipps von Keeper Security zum Umgang mit Cyberbedrohungen

Der Amazon Prime Day ist einer der geschäftigsten Online-Shopping-Events des Jahres und sogleich Hauptziel für Cyberangriffe. Keeper Security verrät wichtige Best Practices, die Kunden helfen, Bedrohungen zu entschärfen und ihre persönlichen Daten zu schützen.

MÜNCHEN, 15. Juli 2024 – Der Amazon Prime Day am 16. und 17. Juli rückt näher und die Online-Kunden bereiten sich auf eine Reihe von Angeboten und Rabatten vor. Der erhöhte Betrieb und die Aufregung rund um dieses globale Shopping-Ereignis ziehen jedoch auch Cyberkriminelle an, die ahnungslose Kunden ausnutzen wollen. Es ist wichtig, dass die Verbraucher wachsam bleiben und ihre Kreditkarten, Konten und persönlichen Daten schützen. Keeper Security, führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang, Geheimnissen und Remote-Verbindungen, informiert über wichtige Best Practices, die helfen, Bedrohungen zu entschärfen und sicher einzukaufen.

Cyberkriminelle entwickeln ständig neue, raffinierte Methoden, um ihre Angriffe auszuführen. Während des Amazon Prime Days grassieren gefälschte Amazon-Benachrichtigungen und Angebote, die die Datensicherheit ahnungsloser Kunden bedrohen. Phishing-Angriffe, Ransomware, Malware, kompromittierte E-Mails und gefälschte QR-Codes zählen zu den gängigen Taktiken, um Verbraucher zu täuschen und hinters Licht zu führen. Um diesen Bedrohungen etwas entgegenzusetzen, sollten die Käufer die folgende Tipps beachten:

- Kaufen Sie nur auf der offiziellen App oder Webseite ein: Betrüger erstellen oft gefälschte Webseiten, welche die Websites bekannter Unternehmen imitieren, um ahnungslose Kunden anzulocken. Um zu vermeiden, dass Sie diesen Betrügern zum Opfer fallen, stellen Sie sicher, dass Sie über die offizielle App oder Website von Amazon einkaufen. Vermeiden Sie es, die Website über Nachrichten oder Links Dritter anzuklicken, da es sich dabei um Betrug handeln könnte. Achten Sie außerdem auf falsche Anzeigen in Suchergebnissen, die Sie zu einer gefälschten Version der legitimen Webseite führen könnten. Zum Beispiel könnte die URL www.Amazon.com leicht verändert werden (z.B. www.Amaz0n.com) und auf eine gefälschte Website führen.

- Hüten Sie sich vor Phishing-Betrug: Da Millionen von Nutzern auf der Suche nach den besten Prime Day-Angeboten sind, könnte es sein, dass Cyberkriminelle E-Mails oder Textnachrichten verschicken, in denen Kunden aufgefordert werden, auf Links zu klicken oder persönliche Daten anzugeben. Diese Links führen häufig zu betrügerischen Websites, die sich als seriöse Einzelhändler ausgeben und Verbraucher mit unglaublichen Angeboten oder Preisen locken. Die Käufer werden möglicherweise aufgefordert, ihre Kreditkarten- oder Kontoinformationen einzugeben, wodurch Cyberkriminelle Zugang zu vertraulichen Daten erhalten würden. Überprüfen Sie immer den Absender einer unaufgeforderten E-Mail, überprüfen Sie URLs, bevor Sie eine Website besuchen, und öffnen Sie keine Anhänge, die Sie nicht erwartet haben - insbesondere nicht von ungeprüften Absendern. Seien Sie vorsichtig bei Nachrichten mit

Tippfehlern, Angeboten, die zu gut sind, um wahr zu sein, oder Aufforderungen zum sofortigen Anklicken von Links, da dies häufige Betrugsanzeichen sind.

- Verwenden Sie sichere und eindeutige Passwörter: Alle Ihre Konten sollten mit sicheren Passwörtern geschützt werden. Ein sicheres Passwort besteht aus mindestens 16 Zeichen und verwendet Groß- und Kleinbuchstaben sowie Zahlen und Symbole. Passwörter sollten für jedes Konto einzigartig sein, denn wenn ein Cyberkrimineller ein Passwort in die Hände bekommt, das für mehrere Konten verwendet wird, kann er auf alle Konten zugreifen. Ein Kennwortgenerator kann sichere Kennwörter für alle Ihre Konten erstellen. Noch besser ist es, wenn ein Passwort-Manager die Passwörter für alle Ihre Konten generiert, speichert und automatisch füllt und gleichzeitig eine eingebaute Warnung vor gefälschten Websites bietet.

- Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA): MFA fügt eine weitere Sicherheitsebene hinzu, da mehrere Überprüfungsmethoden erforderlich sind, bevor der Zugriff auf ein Konto gewährt wird. Dieser zusätzliche Sicherheitsschritt trägt dazu bei, dass Cyberkriminelle selbst dann, wenn ein Passwort kompromittiert wurde, beim Versuch, auf das Konto zuzugreifen, vereitelt werden. Die Aktivierung von MFA ist ein entscheidender Schritt zur Verstärkung Ihrer Abwehrmaßnahmen. Ein sicherer Passwortmanager kann nicht nur sichere Passwörter generieren und speichern, sondern auch Ihre MFA-Codes speichern und automatisch ausfüllen.

„Während die Vorfreude auf den Amazon Prime Day steigt, ist es wichtig, sich daran zu erinnern, dass Cyberkriminelle genauso eifrig darauf aus sind, diesen Event zu nutzen, wie die Käufer auf der Suche nach großartigen Angeboten sind", sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Unser Ziel bei Keeper ist es, unsere Nutzer mit dem Wissen und den Werkzeugen auszustatten, die sie benötigen, um ihre persönlichen Daten vor immer raffinierteren Cyberbedrohungen zu schützen. Denken Sie daran, dass es bei der Cybersicherheit nicht nur um Technologie geht - es geht darum, bewusst und proaktiv seine persönlichen Daten zu schützen."

Um sich zu schützen, ist es unerlässlich, sich über die neuesten Cybersicherheitspraktiken zu informieren. Wenn Sie verstehen, wie wichtig es ist, nur seriöse Websites zu besuchen, auf Phishing-Betrug zu achten, sichere Passwörter zu verwenden und MFA zu aktivieren, kann dies Ihre Sicherheit erheblich verbessern. Grundsätzlich ist es besser, skeptisch zu sein, da Cyberkriminelle Schwachstellen gerne ausnutzen.

Wenn Sie diese Schritte befolgen, können Sie die Angebote und Rabatte des Amazon Prime Days genießen und sich gleichzeitig sicher sein, dass Ihre Daten geschützt bleiben. Lassen Sie nicht zu, dass Cyberkriminelle ein tolles Angebot in einen teuren Betrug verwandeln.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: 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