KEEPER | Pressemitteilung

Black Friday: Wie man gute Online-Schnäppchen macht, ohne seine persönlichen Daten zu riskieren

Der Black Friday ist oft gleichbedeutend mit attraktiven Angeboten und vollen Warenkörben. Aber diese Zeit ist ebenso attraktiv für Cyberkriminelle, die auf einfache Beute aus sind. Keeper gibt 7 Tipps, wie die Schnäppchenjagt sicher bleibt.

Der Black Friday läutet die Weihnachtseinkaufssaison ein, in der Händler mit Rabatten um die Gunst der Online-Kunden buhlen. Doch hinter den verlockenden Angeboten und auffälligen Bannern können Cyberbedrohungen lauern. Die mannigfaltigen Angebote auf Online-Shopping-Plattformen zieht auch Hacker an, die versuchen Konten zu hacken, Bankdaten zu stehlen oder auf betrügerische Links zu locken. So stark die Versuchung eines Angebots auch sein mag, es ist und bleibt wichtig, einige Sicherheitsmaßnahmen zu beachten, damit aus einem guten Geschäft kein digitaler Albtraum wird.

1. **Wählen Sie Ihre Websites sorgfältig aus:** Angesichts der Angebotsflut passiert es leicht, auf den ersten Link oder die nächste Anzeige zu klicken. Doch nicht alle Websites sind in Sachen Sicherheit gleich. Bevorzugen Sie bekannte Anbieter, recherchieren Sie renommierte Marken und achten Sie darauf, dass die URL mit „https“ beginnt, um einen Mindestschutz der Daten zu gewährleisten.

2. **Aktualisieren Sie Ihre Geräte:** Cyberangriffe nutzen oft Sicherheitslücken in nicht aktualisierten Systemen oder Anwendungen aus. Stellen Sie sicher, dass Ihr Telefon, Computer und alle Anwendungen auf dem neuesten Stand sind, bevor Sie mit dem Einkaufen beginnen. Mit den neuesten Versionen des Betriebssystems und der Antivirenprogramme stärken Sie Ihre Online-Sicherheit.

3. **Schützen Sie Ihre Passwörter:** Jeder Onlineshop erfordert ein eigenes Konto. Oft werden dafür aber dieselben Passwörter mehrfach verwendet. Doch diese Angewohnheit öffnet Cyberkriminellen Tür und Tor. Nutzen Sie für jede Seite einzigartige und komplexe Passwörter und verwenden Sie nach Möglichkeit einen Passwort-Manager, um die Verwaltung zu erleichtern und die Sicherheit zu erhöhen.

4. **Bevorzugen Sie sichere Zahlungsmethoden:** Beim Online-Shopping geben Sie auch Bankdaten preis. Wählen Sie Zahlungsmethoden, die Sicherheit bieten, wie Kreditkarten oder sichere Bezahldienste (wie PayPal). Um zu vermeiden, dass Ihre Kartendaten leicht zugänglich bleiben, speichern Sie diese nicht direkt auf den Websites und teilen Sie niemals Ihre Bankdaten per E-Mail oder Nachricht.

5. **Vorsicht bei Angeboten, die zu gut sind, um wahr zu sein:** Cyberkriminelle wissen, wie sie mit Gefühlen spielen, indem sie übermäßig verlockende Angebote präsentieren. Seien Sie misstrauisch bei unrealistischen Rabatten oder bei Angeboten, die Sie unter Druck setzen, beispielsweise indem der Vorrat begrenzt ist. Wenn Ihnen eine Website verdächtig erscheint, überprüfen Sie die Echtheit des Angebots, bevor Sie darauf klicken.

6. **Aktivieren Sie Anti-Phishing-Warnungen:** Die Zeiten intensiven Konsums sind ideal für Phishing-Versuche. Um nicht in die Falle zu tappen, lernen Sie, verdächtige E-Mails zu erkennen. Grammatikfehler, schlecht reproduzierte Logos oder seltsame Links

können Indizien sein. Wenn Sie ein Angebot per E-Mail erhalten, klicken Sie nicht sofort darauf, sondern besuchen Sie die offizielle Website über eine Suchanfrage.

7. **Vermeiden Sie öffentliche WLANs:** Gratis-WLAN ist praktisch, aber wenig sicher. Für sichereres Einkaufen nutzen Sie besser das heimische Netzwerk oder Ihre mobile Verbindung. Öffentliche Netzwerke könnten Ihre sensiblen Daten ungewollt Hackern preisgeben, die den Datenverkehr der Nutzer beschatten.

Indem Sie diese Tipps am Black Friday beherzigen, können Sie das Schnäppchenjagen entspannt genießen und gleichzeitig Ihre persönlichen und finanziellen Daten schützen.

###

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