

Cyber Week: Die versteckten Risiken

Die Cyber-Week ist jedes Jahr ein Höhepunkt für Online-Käufe und Händler. Ursprünglich als Erweiterung des Black Fridays für den Onlinehandel entstanden, hat sich die Cyber-Week zu einer globalen Shopping-Woche entwickelt. Doch wo Chancen liegen, gibt es auch Risiken. Besonders in dieser Woche sollten Privatpersonen und Unternehmen wachsam bleiben, denn der digitale Boom zieht nicht nur Käufer an.



Foto: Pixabay

Welche Gefahren verbergen sich?

Der Nachteil der Cyber-Week sind die zunehmenden Aktivitäten von Cyberkriminellen, die die hohe Kaufaktivität online gezielt ausnutzen, warnt die *Konvert*. Zu den häufigsten Gefahren gehören:

- **Fake-Webshops:** Professionell gestaltete, aber gefälschte Websites locken Kunden mit unschlagbaren Angeboten. Sobald die Zahlungsdaten eingegeben wurden, verlieren Käufer Geld und persönliche Daten.
- **Phishing-Mails:** Betrügerische E-Mails nehmen in der Cyber-Week stark zu. Diese imitieren bekannte Händler oder Banken, um an sensible Daten zu gelangen.
- **Malware in Angeboten:** Kostenlose Downloads, die als Gutscheine oder Rabattcodes ausgegeben werden, können eine Schadsoftware, die Geräte infiziert und Daten stiehlt.

Data: 02/12/2024

Categoria: Raiffeisen-Geldorganisation Print & Web | [Link](#)

- **Datenlecks:** Auch Unternehmen stehen unter Druck: Angreifer nutzen Sicherheitslücken aus, um auf sensible Kundendaten oder Geschäftsinformationen zuzugreifen.

Wie können Sie sich schützen? Konverto gibt Tipps:

Privatpersonen:

Beim Online-Einkauf ist Vorsicht geboten. Angebote sollten sorgfältig geprüft werden, da Websites mit unrealistisch günstigen Produkten häufig betrügerisch sind. Es ist ratsam, nur bei seriösen Anbietern zu kaufen und sichere Zahlungsmethoden wie PayPal oder Kreditkarten mit Käuferschutz zu verwenden. Darüber hinaus sollte stets eine sichere Internetverbindung genutzt werden – öffentliches WLAN birgt ein erhöhtes Risiko. Ebenso wichtig ist der Schutz der eigenen Geräte durch aktuelle Antivirensoftware und regelmäßige Updates.

Unternehmen:

Auch Unternehmen müssen sich rüsten und proaktiv handeln, um ihre IT-Infrastruktur zu sichern. Ein verstärktes Sicherheitsbewusstsein ist essenziell. Dazu gehören regelmäßige Schulungen für Mitarbeiter zum Erkennen von Phishing-Angriffen, der Schutz der Netzwerke durch Firewalls sowie die Durchführung von Sicherheits-Updates und Backups. Eine umfangreiche IT-Sicherheitsstrategie ist nicht nur eine Absicherung gegen Cyberangriffe, sondern optimiert gleichzeitig die digitale Infrastruktur und schützt die Kundendaten effektiv.

Jetzt **Teilen**, **Tweet** oder mit **WhatsApp** versenden.

Folge uns auf Instagram!
Immer aktuell informiert! www.instagram.com/unsertirol24

DISKUTIEREN SIE MIT

Sie müssen **eingeloggt** sein, um einen Kommentar zu schreiben.

NEUESTE MELDUNGEN



SÜDTIROL

Acht Gewehre sichergestellt:
Familie im Vinschgau im Visier
der Polizei

02.12.2024



ÖSTERREICH

Aufruf zur Wintervögel-
Zählung ab 4. Jänner

02.12.2024



WELTSCHTIROL

VVF, nel 2024 già 2800
interventi

02.12.2024
