

Achtung Urlauber! So betrügen Online-Betrüger bei der ETA-Anmeldung

Betrüger zielen auf Urlauber, indem sie gefälschte ETA-Anträge anbieten. Achten Sie auf offizielle Seiten und schützen Sie Ihre Daten.



Großbritannien - Am 4. April 2025 ist die Einreise nach Großbritannien für EU-Bürger in Verbindung mit einer digitalen Reisegenehmigung (ETA) geregelt worden. Das Österreichische Bundeskriminalamt (BKA) warnt nun vor betrügerischen Machenschaften, die es auf ahnungslose Urlauber abgesehen haben, berichtet **5min.at**. Mit dem Inkrafttreten dieser neuen Regelung am 2. April ist die digitale Reisegenehmigung erforderlich, die online oder über eine App beantragt werden kann. Die Kosten für die ETA betragen etwa 12 Euro, sie ist für zwei Jahre gültig und erlaubt mehrfache Einreisen mit einem Aufenthalt von bis zu drei Monaten.

Airlines sind verpflichtet, vor dem Boarding sicherzustellen, dass

die Reisenden im Besitz der ETA sind. Dies bietet jedoch eine neue Angriffsfläche für Betrüger, die gefälschte Websites erstellen, um persönliche Daten und Kontoinformationen zu stehlen. Die Masche umfasst häufig die Aufforderung an die Opfer, ihre Reisepassdaten und Kontoinformationen zur Begleichung der ETA-Gebühr hochzuladen. Hierbei verlieren die Betroffenen oft mehrere Hundert Euro, zwischen 200 und 900 Euro können von ihren Konten abgebucht werden. Das BKA beschreibt dieses Vorgehen als klassisches Phishing.

Tipps zur Betrugsprävention

Um sich vor solchen Betrügereien zu schützen, empfiehlt das BKA folgende Maßnahmen:

- Suche nach der offiziellen ETA-Website unter www.gov.uk/eta.
- Achte auf den Abbuchungsbetrag auf deinem Konto.
- Überprüfe Links, bevor du darauf klickst.

Wenn du Opfer eines Betrugs geworden bist, solltest du umgehend Anzeige bei der Polizei erstatten und das Gerät, auf dem der Betrug erfolgte, zur Anzeige mitbringen. Zudem ist es notwendig, die Bank über ungerechtfertigte Abbuchungen zu informieren.

Das wachsende Betrugsrisiko im E-Commerce

Die neue Reisegenehmigung ist nicht das einzige Thema, das potenzielle Opfer betrifft. Das Wachstum des elektronischen Handels steigert das Risiko von Online-Betrug erheblich. Laut einer Analyse von **Stripe** wird prognostiziert, dass die weltweiten Kosten des Online-Zahlungsbetrugs bis 2025 auf 206 Milliarden USD steigen. Zwischen 2023 und 2027 könnten Unternehmen mehr als 343 Milliarden USD durch Online-Betrug verlieren.

Typische Betrugsarten im Online- und E-Commerce-Bereich reichen von Phishing, bei dem gefälschte E-Mails zur Erlangung vertraulicher Informationen versendet werden, bis hin zu Identitätsdiebstahl. Betrüger entwickeln kontinuierlich neue Taktiken, um Sicherheitsmaßnahmen zu umgehen und ahnungslose Nutzer zu täuschen. Besonders gefährdet sind Unternehmen, die mit sensiblen Daten arbeiten. Kleine Unternehmen sind oft weniger gut geschützt als größere Konzerne und deshalb häufig Ziel von Angriffen.

Statistiken zeigen, dass die pandemiebedingte Zunahme von Online-Transaktionen um 20% dazu führt, dass Betrüger immer aggressiver vorgehen. Es ist daher wichtig, dass E-Commerce-Unternehmen die Bedrohung durch Betrug ernst nehmen und einen mehrschichtige Sicherheitsansatz implementieren, der moderne Authentifizierungstechnologien und effiziente Betrugserkennungslösungen einschließt.

Details	
Vorfall	Betrug
Ort	Großbritannien
Quellen	• www.5min.at • stripe.com

Besuchen Sie uns auf: die-nachrichten.at