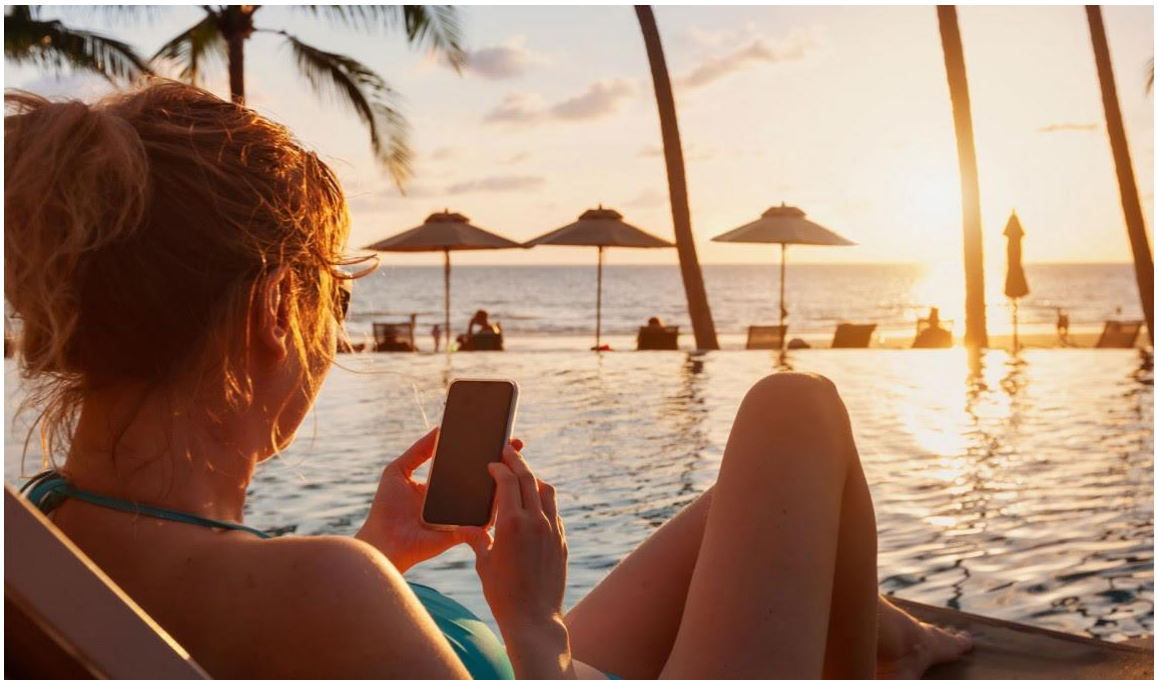
Roaming und Phishing können teuer werden

Mobile Daten auf Reisen sind angenehm für Musik, Chatten oder Streamen. Doch teure **Roaming-Gebühren** können im Auslaund zur Kostenfalle werden. Wir haben Tipps für Sie!

Haben Sie auch schon mal zur "falschen" Packung im Supermarkt gegriffen? **Verdorbenes Obst und Gemüse** im Netz oder Plastikverpackung sind ärgerlich und teuer. Der AK-Konsumentenschutz hat die Supermärkte in Oberösterreich unter die Lupe genommen: das Ergebnis fällt schlecht aus.

Online-Betrüger versuchen mit seriösen Botschaften Geld aus Ihrer Tasche zu angeln. Wir zeigen Ihnen, wie Sie sich vor **Phishing-Versuchen** schützen und was Sie im Notfall tun können.

Die Konsumentenschützer:innen wünschen Ihnen ein schönes Wochenende!



© Song_about_Summer

TELEFON

Roaming auf Reisen: vor Kostenfalle schützen

Chatten, surfen und lange Telefongespräche auf Reisen: Das Smartphone kann im Urlaub teuer werden. Informieren Sie sich über versteckte Kosten fürs Handy im Ausland.

So schützen Sie sich →

© pressmaster

ERNÄHRUNG

Obst und Gemüse: Faule Früchtchen im Regal

Konsument:innen erleben immer wieder nach dem Einkauf, dass Obst und Gemüse im Netz oder in einer Plastikschale bereits verdorben ist. Wir haben uns die Ware in oberösterreichischen Supermarktregalen genauer angeschaut: Das Ergebnis fällt schlecht aus.

So schneiden die Supermärkte ab →

© davidevison

INTERNET

Phishing und Trojaner

Immer wieder werden im Internet Kundendaten von User:innen gestohlen. Mit scheinbar seriösen E-Mails versuchen Kriminelle sensible Daten abzugreifen, um damit Profit zu machen. Wir haben Tipps für Sie.

Das sollten Sie beachten →

Phishing und Trojaner - so schützen Sie sich!

Phishing, der Diebstahl von Kundendaten im Internet, bedroht nach wie vor User/-innen, die im Netz einkaufen oder Online-Banking nutzen. Mails mit Trojanern, dabei wird schädliche Software auf den PC installiert, landen in fast jedem Mailordner.

Vorsicht bei scheinbar seriösen E-Mails

Jeder kennt E-Mails, die anscheinend von einem vertrauenswürdigen Unternehmen, einer Institution bzw. Anwaltskanzlei stammen. In denen wird gefordert, einem Link zu folgen bzw. die angefügte Rechnung zu öffnen. Entweder soll eine Bestellung/Mitgliedschaft bestätigt, das **PayPal-, Kreditkarten**- oder **Bankkonto** überprüft oder eine Zahlung getätigt werden.

Werden Sie aufgefordert vertrauliche Daten **(IBAN, PIN, TAN** oder **Kennwörter)** bekannt zu geben, handelt es sich um ein Phishing-Mail. Mit diesen Daten kann finanzieller Schaden entstehen.

TIPP

Öffnen Sie keine verdächtigen Mails oder deren Anhänge, etwa wenn Sie mit der Firma noch nie Kontakt hatten oder die Nachricht in einer fremden Sprache verfasst oder fehlerhaft ist. Seriöse Unternehmen wie Banken und Kreditkartenunternehmen fragen niemals von Ihnen via E-Mail oder Telefon sensible Daten (Kontodaten, PIN, TAN oder Kennwörter) ab. Wenn Sie Ihre Daten kontrollieren, loggen Sie sich direkt auf der Homepage der Firma ein. Den mitgeschickten Link nicht verwenden.

Technischer Schutz vor Phishing

Verwenden Sie ein aktuelles Betriebssystem, ein Anti-Virenprogramm und eine Firewall. Führen Sie Sicherheitsupdates für alle diese Programme sowie für Ihren Internet-Browser durch.

Falls Sie WLAN verwenden, sollten Sie die Übertragung verschlüsseln. **Bankgeschäfte** sollten keinesfalls auf fremden Rechnern vorgenommen werden. Keinesfalls sollten **sensible Daten** an öffentlich zugänglichen Rechnern oder „Hotspots“ eingegeben werden.

Geben Sie Daten soweit möglich nur auf sicheren Seiten (https://) ein. Achten Sie auf Pop-Up-Fenster, die die Eingabe von Daten vor der eigentlichen Anmeldung verlangen oder sich vor der echten Seite öffnen und schließen Sie diese.

Wenn Sie von Phishing betroffen sind

1. Teilen Sie umgehend Ihrer Bank mit, dass Sie Opfer von Phishing wurden und verlangen Sie, dass die illegale Transaktion rückgängig gemacht wird. Allerdings kann Ihre Bank unter Umständen diesen Anspruch reduzieren oder die Rückzahlung ganz verweigern, wenn Sie Ihre „personalisierten Sicherheitsmerkmale“ (also insbesondere PIN und TAN) nicht sicher aufbewahrt oder Ihren Rechner nicht ausreichend gegen Datendiebstahl gesichert haben.

2. Ändern Sie Ihre Zugangsdaten und Kennwörter.

3. Wurden Sie geschädigt, sollten Sie auch Strafanzeige erstatten und dabei das (gesicherte) verdächtige E-Mail vorlegen.

Absender von gefälschten Mails sind bzw. Trojanerverdacht besteht bei:

- A1 Service Team
- LIWEST
- Amazon
- FinanzGruppe Volksbanken Raiffeisenbanken
- DHL
- Telekom Deutschland
- Vodafone
- NTTcable
- BrandtOnline GmbH
- KochOnline GmbH
- ZieglerNet GmbH
- JungOnline GmbH
- BaumannOnline GmbH
- Heartbooker
- Walter GmbH
- Meyer GmbH
- Meier GmbH
- Bauer GmbH
- Herbert GmbH
- Rechtsanwalt Bank Payment
- Willhaben
- ...

INHALT

DAS KÖNNTE SIE AUCH INTERESSIEREN

Internetbetrug

Betrügerische Aktivitäten gibt es im Internet genauso wie im restlichen Leben. Vermeintliche Anonymität bietet Nährboden für Kriminalität.