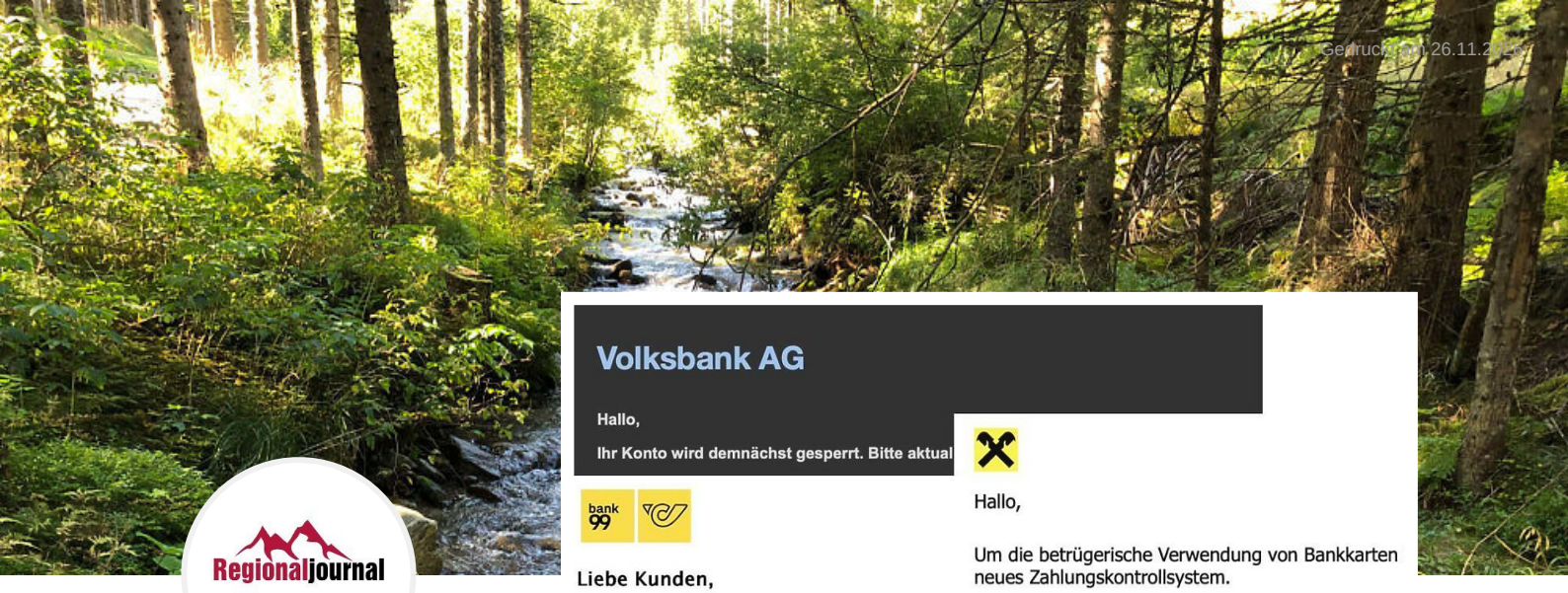

Regionaljournal Steiermark

Aktuelle Phishing- und Betrugsversuche

Die Zahl sogenannter Phishing Nachrichten (E-Mails, SMS, Messenger Nachrichten) und Schadsoftware auf Websites steigt stetig an. Um Sie bestmöglich vor Gefahren im Internet zu schützen, finden Sie hier einige Tipps und Musterbeispiele zum Thema Gefahren im Internet.

Die Tricks von Online-Kriminellen werden immer raffinierter. Phishing E-Mails sind oft täuschend echt. Scheinbar vertrauenswürdige Websites enthalten Schadsoftware oder verfolgen Betrugsabsichten. Erst bei genauem Hinschauen erkennt man die Tricks der Kriminellen. Wir geben Ihnen Tipps für Ihren Alltag, damit Sie gut geschützt im Internet unterwegs sind. So warnt die Post aktuell wieder verstärkt:

Seien Sie achtsam bei Aufforderungen zur Dateneingabe, insbesondere bei Zugangsdaten, Zahlungs- und Adressinformationen

- Nutzen Sie Online Services und Empfangsoptionen ausschließlich über Ihren Post Account.
- Führen Sie Änderungen (z.B. Benutzername, E-Mail-Adresse, Passwort) an Ihrem Post Account direkt über die Post App oder unsere Webseite www.post.at durch.
- Verifizieren Sie Zahlungsaufforderungen per E-Mail durch Kontrolle der Sendungs- und Bestellnummern.

Schauen Sie genau hin, ob das E-Mail oder SMS tatsächlich von der Österreichischen Post AG versendet wurde

- Überprüfen Sie die Sendungsnummer in der offiziellen Sendungsverfolgung der Post – in der Post App oder auf **post.at/sendungsverfolgung**.
- Lassen Sie sich nicht von gefälschten Webseiten oder E-Mails im Post-Design oder im Namen der Post täuschen. Sehen Sie sich die

Webadresse bzw. die E-Mail-Adresse genau an. Wir verwenden ausschließlich die Endung post.at.
- Rechtschreibfehler, verpixelte Logos und kryptische Absender*innen von E-Mails sollten alle Alarmglocken läuten lassen.

Hinterfragen Sie Gewinnspiele, Schein- und Lockangebote kritisch

- Die Österreichische Post AG verlost bzw. verkauft keine Mystery-Pakete oder Retourenpaletten.
- Fragen Sie bei dem*der Absender*in nach, wenn nur die Versandart „Nachnahme“ angeboten wird.

Schützen Sie Ihren Post Account

- Verwenden Sie ein sicheres Passwort (mind. 10-stellig, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) oder einen Passwortmanager.
- Ändern Sie Ihr Passwort in regelmäßigen Abständen.
- Achten Sie auf unbekannte Vorgänge in Ihrem Post Account (z.B. werden Sendungen angezeigt, die Sie nicht bestellt haben)

Was tun im Falle des Betrugsverdachtes?

Bitte nehmen Sie umgehend mit unserem **Post-Kundenservice** Kontakt auf.

Tipps zur Erkennung von Fake-Websites

- Unternehmensseiten sind verpflichtet, ein gültiges Impressum auf ihrer Webseite zu veröffentlichen. Prüfen Sie im Menü (z.B. unter Info) oder am unteren Ende der Seite (Footer), ob sie einen Link zu einem Impressum finden.
- Auf der Seite **Watchlist Internet** können Sie nachlesen, ob ein (ähnlicher) Betrugsfall bereits vorliegt.

Tipps zur Erkennung von Fake-Facebook-Gewinnspielen

- Offizielle und verifizierte Unternehmensseiten sind am blauen Häkchen erkennbar.
- Unternehmensseiten sind verpflichtet, ein gültiges Impressum anzugeben. Sehen Sie nach, ob auf der Facebook Seite ein Link zu einem Impressum zu finden ist.
- Achten Sie auf Teilnahmebedingungen. Facebook-Gewinnspiele müssen einen Link zu Teilnahmebedingungen aufweisen.