Achtung, Spotify-Nutzer! So schützen Sie sich vor perfiden Phishing-Mails!

Betrüger zielen auf Spotify-Nutzer: Phishing-Mails bedrohen persönliche Daten. Verbraucherschutz gibt wichtige Tipps zur Abwehr.

Deutschland - Aktuell warnen Verbraucherschutzorganisationen vor einer neuen Welle von Phishing-Attacken, die gezielt auf Spotify-Nutzer abzielen. Betrüger verschicken gefälschte E-Mails, die fälschlicherweise behaupten, das Spotify-Abo sei aufgrund einer überfälligen Zahlung vorübergehend pausiert worden. Diese Mails sind gut gemacht und täuschen den Eindruck von Authentizität vor. So wird in den Nachrichten von der **tz** berichtet, dass die E-Mails darauf abzielen, persönliche Daten sowie Zahlungsinformationen abzugreifen.

Eine typische E-Mail könnte den Empfänger auffordern, auf einen Link zu klicken, um die Zahlungsinformationen zu aktualisieren. Dieser Link führt allerdings zu einer gefälschten Webseite, die dem echten Spotify-Auftritt ähnelt und lediglich darauf ausgelegt ist, Log-in- und Kreditkartendaten zu stehlen. Das Verbraucherschutzportal „Watchlist Internet“ warnt eindringlich, dass Nutzer in solchen Fällen definitiv keine Links in den Mails anklicken sollten.

Merkmale gefälschter E-Mails

Die Phishing-Mails weisen einige charakteristische Merkmale auf. Viele enthalten unpersönliche Anreden und die Absenderadresse ist oft leicht abgeändert, was ein deutliches

Zeichen für Betrug ist. Spotify selbst kommuniziert ausschließlich über die Domain „spotify.com“ und spricht Kunden mit Namen an. Zudem werden von Spotify keine Zahlungsaufforderungen per E-Mail verschickt; stattdessen wird lediglich zur Aktualisierung von Zahlungsinformationen aufgefordert.

Verbraucherschützer warnen zudem, dass solche betrügerischen E-Mails oft mit Drohungen kommen, etwa dass das Konto gesperrt wird, wenn die якkelte Zahlung nicht fortgesetzt wird. Nutzer sollten im Zweifel die offizielle Webseite von Spotify direkt im Browser aufrufen, anstatt auf Links in verdächtigen E-Mails zu klicken. Wenn jemand bereits sensible Daten eingegeben hat, ist es ratsam, sofort das Passwort zu ändern und auch die Banken zu informieren.

Schutzmaßnahmen gegen Phishing

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet umfassende Informationen darüber, wie man sich gegen Phishing-Angriffe schützen kann. Ein zentraler Ratschlag ist, niemals persönliche Zugangsdaten oder Zahlungsinformationen über E-Mail zu übermitteln. Weitere Tipps sind, die Adresszeile des Browsers im Auge zu behalten und häufig besuchte Login-Seiten als Lesezeichen zu speichern. Darüber hinaus sollte man regelmäßig die Kontostände überprüfen und verdächtige E-Mails umgehend an den Anbieter weiterleiten.

Zusätzlich rät das BSI, keine Dateianhänge von unbekannten oder dubiosen Absendern zu öffnen und Downloads nicht direkt aus E-Mails zu starten, deren Echtheit unklar ist. Nutzer sollten zudem sicherstellen, dass ihre Antivirensoftware aktuell ist und die Firewall aktiviert ist, um sich bestmöglich abzusichern. Für detaillierte Informationen zum Thema Phishing und damit verbundenen Sicherheitsmaßnahmen können Nutzer die Webseite des BSI besuchen: **BSI**.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Deutschland
Quellen	• **www.tz.de** • **www.wa.de** • **www.bsi.bund.de**