KRIMINAL PRÄVENTION POLIZEI

Sehr geehrte Bürgerin, sehr geehrter Bürger!

GEMEINSAM.SICHER in Österreich

Vorsicht bei Amazon-Betrug - Vorsicht vor Fake-Amazon-Anrufen!

Aufgrund aktuell vermehrter angezeigter Fälle in der Gemeinde Riegersburg wird vor dieser Betrugsmasche gewarnt!

Die übliche Vorgehensweise:

Am Telefon geben sich Kriminelle als Amazon-Mitarbeiter:innen aus. Unter verschiedenen Vorwänden bringen sie Sie dazu, die Software TeamViewer oder AnyDesk zu installieren und räumen Ihr Konto leer!

Sollten Sie so einen Anruf erhalten, legen Sie auf und blockieren Sie sofort die Nummer.

Wie laufen die Fake-Anrufe ab?

Ihr Telefon klingelt - es ist eine österreichische Nummer. Die Person am anderen Ende der Leitung stellt sich als Amazon Mitarbeiter:in vor. Sie erklärt, dass es ein Problem mit einer Bestellung oder Ihrem Konto gibt. Vielleicht ist sogar von einem Betrugsversuch die Rede. Um die Geschichte zu untermauern, wird eine angebliche Mitarbeiternummer genannt oder Sie werden zu einem angeblichen Vorgesetzten durchgestellt.

Um den vermeintlichen Betrugsversuch zu verhindern oder das Problem zu beheben, werden Sie aufgefordert, eine Remote Desktop Control Software AnyDesk zu installieren. Es wird behauptet, dass Ihnen die Mitarbeiter:innen durch die Installation dieser Fernwartungssoftware besser bei der Lösung des Problems helfen können. Über diese Remote Desktop Control oder Fernwartungssoftware wie AnyDesk kann Ihr Gerät (Smartphone oder Computer) von anderen Personen gesteuert und eingesehen werden.

Danach werden Sie angeleitet, sich in Ihrem Amazon-Konto einzuloggen. So bekommen die Kriminellen Zugriff auf Ihr Amazon-Konto. Weiters werden Sie aufgefordert, Ihre Online-Banking-App (z.B. George - Erste Bank oder Mein ELBA - Raiffeisenbank) zu öffnen, um einen angeblichen Hackingangriff zu stoppen. Allerdings erlangen die Kriminellen so Zugang zu Ihrer Banking-App und können anschließend auch Ihr Konto leerräumen.

So erkennen Sie betrügerische Anrufe:

- Amazon ruft nur an, wenn Sie es anfordern.
- Service-Mitarbeiter:innen fragen nicht nach persönlichen Daten, Passwörtern, Bank- oder Zahlungsdaten.
- Amazon fordert Sie niemals telefonisch auf, eine Überweisung vorzunehmen. Das ist ein eindeutiges Zeichen für Vishing.
- Amazon bittet Sie nicht, Programme oder Apps wie AnyDesk herunterzuladen. Amazon würde auch niemals mit einer Wartungssoftware oder Remote Desktop Control auf Ihr Gerät zugreifen.
- Legen Sie einfach auf, wenn Sie ein komisches Gefühl haben!

Sie sind in die Falle getappt? Das ist jetzt zu tun:

- Wenn Sie Zahlungen freigegeben oder Bankdaten übermittelt haben, sollten Sie umgehend Ihre Bank kontaktieren. Die Mitarbeiter:innen wissen was zu tun ist.
- Ändern Sie Passwörter, falls Sie diese übermittelt haben oder falls Sie sich in Ihr Amazon-Konto bzw. Ihre Banking-App eingeloggt haben!
- Entfernen Sie die installierten Programme wie AnyDesk. Möglicherweise haben die Kriminellen auch eine Spionage-Software installiert. Dann sollten Sie Ihr Gerät neu aufsetzen. Das können Sie tun, wenn Ihr Gerät mit Schadsoftware infiziert wurde.
- Melden Sie den Fall an Amazon. Schicken Sie die Falle bzw. Ihren Erfahrungsbericht an stop-spoofing@amazon.com.
- Erstatten Sie eine Anzeige bei der Polizei.

LINKS:

https://www.watchlist-internet.at/news/amazon-vishing-vorsicht-vor-fake-amazon-anrufen/

https://www.amazon.de/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B