Neuer raffinierter Betrug im Umlauf

Uns hat in der letzten Woche eine interessante Spam-Mail erreicht, ein neuer Betrugsversuch. Die Internetkriminellen lassen sich immer neue Tricks einfallen, um an unser Geld oder an unsere Daten zu kommen. Dabei versuchen sie oft, uns zu locken, unsere Neugierde oder unsere Gier zu wecken. So funktioniert auch die neuste Masche, doch sehen Sie selbst. Hier ein Bild dieser Mail:

ARD ZDF Deutschlandradio

BEITRAGSSERVICE

Wichtige Rückerstattungsbenachrichtigung

Sehr geehrte Kundin, sehr geehrter Kunde,

Wir möchten Sie darauf hinweisen, dass wir noch keine Antwort auf unsere vorherige Anfrage erhalten haben. Es ist wichtig, dass Sie sich umgehend bei uns melden, um etwaige Fragen zu klären.

Falls Ihnen eine Rückerstattung zusteht, sei es aufgrund einer Überzahlung oder eines Fehlers bei der Buchung, stellen wir sicher, dass alles ordnungsgemäß bearbeitet wird.

Klicken Sie bitte auf den folgenden Link, um den aktuellen Status Ihrer Rückerstattung zu überprüfen und Ihre Informationen auf dem neuesten Stand zu halten.

Rückerstattungsstatus überprüfen

Mit freundlichen Grüßen,
Ihr Kundenservice-Team

Kundenservice Abteilung
Ihre Firma AG
98765 Ihre Stadt
Telefon: 0123456789
E-Mail: support@ihrefirma.de

Es wird also behauptet, dass eine **Rückzahlung der Rundfunkgebühren** auf uns wartet. Wer möchte nicht gerne davon profitieren und sich Geld zurückholen? Es gibt viele ähnliche Fälle, in denen Betrüger versuchen, sensible Daten von Personen zu stehlen, indem sie Rückzahlungen, Gewinne oder sonstige Geldleistungen versprechen. Diese Masche funktioniert, weil sie oft den Anschein erweckt, von einer vertrauenswürdigen Quelle zu kommen, wie zum Beispiel einer Behörde, einer Bank oder einer bekannten Organisation.

Ähnliche Fälle

Es gibt zahlreiche ähnliche Fälle, bei denen die Betrüger sich als jemand anderes ausgeben um uns dazu zu bringen, aktiv zu werden und Daten preiszugeben:

Steuerrückzahlungen: Betrüger geben vor, von Finanzämtern oder Steuerbehörden zu sein, und versprechen Rückzahlungen. Sie fordern die Opfer auf, ihre Bankdaten oder persönliche Informationen einzugeben.

Gewinnspiele: E-Mails behaupten, dass der Empfänger einen Preis gewonnen hat und dass er nur noch schnell seine Bankdaten oder einen Identitätsnachweis angeben muss, um den Gewinn zu erhalten.

Paketzustellung: In manchen Fällen geben sich Betrüger als Paketdienstleister aus und behaupten, dass ein Paket auf eine zusätzliche Zahlung oder Bestätigung wartet. Über diesen Trick haben wir schon mehrfach berichtet, die Nachrichten werden oft auch per SMS versendet.

Rückzahlungen von Dienstleistern: Wie in unserem Fall mit den Rundfunkgebühren, gibt es auch Fälle, bei denen angebliche Rückzahlungen von Mobilfunkanbietern, Stromversorgern oder Versicherungen in Aussicht gestellt werden.

Worauf haben es die Betrüger abgesehen?

Die Internetkriminellen wollen, je nach Betrugsmasche, verschiedene Informationen von uns erbeuten. Dazu zählen vor allem:
Persönliche Daten: Name, Adresse, Geburtsdatum, E-Mail-Adressen – diese Daten können für Identitätsdiebstahl genutzt werden.
Bankdaten: Betrüger können damit versuchen Geld, von unserem Konto abzubuchen oder betrügerische Überweisungen zu tätigen.
Kreditkartendaten: Diese können im schlimmsten Fall direkt verwendet werden, um unberechtigte Zahlungen durchzuführen.
Login-Daten zu diversen Online-Konten: Wenn die Betrüger Zugang zu Online-Banking- oder anderen Konten wie PayPal, Amazon etc. erhalten, können sie noch weitreichendere (finanzielle) Schäden verursachen.

Wie funktioniert die Masche?

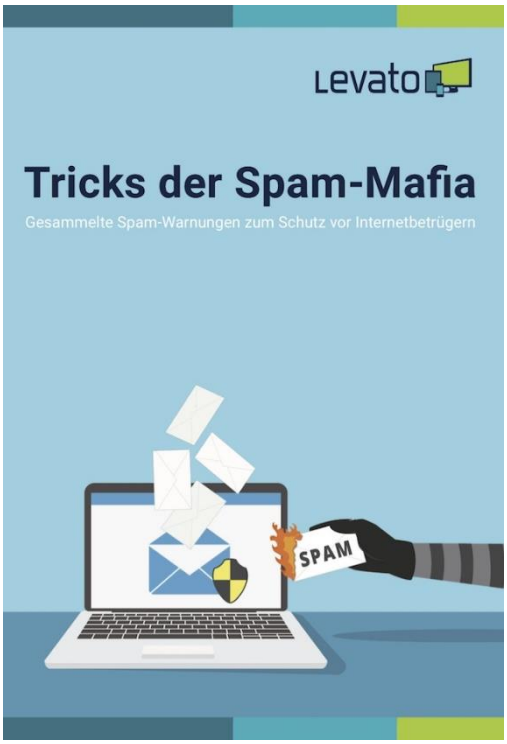
Die Masche beginnt oft mit einer gefälschten E-Mail oder SMS, die täuschend echt aussieht. Sie verwendet meistens Logos, Schriftarten und Sprache, die der echten Organisation oder Firma ähneln. Der Empfänger wird dazu aufgefordert, auf einen Link zu klicken oder eine Webseite zu besuchen, die dann oft nach vertraulichen Daten fragt. Die Webseite kann dabei so gestaltet sein, dass sie wie die offizielle Seite des Unternehmens oder der Behörde aussieht. Sobald die Daten eingegeben werden, gelangen sie direkt zu den Betrügern.

Daher: Betrachten Sie E-Mails, in denen Ihnen irgendein Gewinn oder eine Rückzahlung versprochen wird, immer kritisch. Das Gleiche gilt für Mails, in denen Sie unter Druck gesetzt werden. Löschen Sie verdächtige Mails sofort, klicken Sie keine Links an und antworten Sie auch nicht darauf.

Wir haben über ähnliche Fälle schon häufig berichtet und haben auch ein Buch über die Maschen der Spam-Betrüger geschrieben, es heißt “Die Tricks der Spam-Mafia” und ist in

unserem Shop verfügbar

Tricks der Spam-Mafia



In unserem Lehrbuch finden Sie die typischen Tricks der Spam-Kriminellen. Wir haben dutzende betrügerische E-Mails analysiert und kategorisiert. In 6 Kapiteln stellen wir unterschiedliche Methoden der Betrüger vor, jeweils mit bebilderten Beispielen. In einem siebten Kapitel verraten wir Tipps und Tricks, wie man Spam-Mails erkennt und was man dagegen tun kann.

Sie können das Buch aber auch als Nachschlagewerk für den Notfall benutzen. Sie legen es neben den Computer und wenn eine fragwürdige Mail in Ihrem Posteingang auftaucht, schlagen Sie einfach nach. Weitere Informationen zum Buch finden Sie hier.

Wichtiger aber: Das Buch vermittelt Ihnen ein Gespür, einen Riecher für die Spam-Mails, sodass Sie sich zukünftig ganz alleine schützen können.

Quelle: https://levato.de/neuer-raffinierter-betrug-im-umlauf/?utm_source=mailpoet&utm_medium=email&utm_source_platform=mailpoet&utm_campaign=Raffinierte%20Betrugsmasche%20im%20Umlauf