Internetbetrug: So schützen Sie sich!

eine Sendung von KlagemauerTV

Quelle: KlagemauerTV

Zum Anschauen der Sendung auf das Bild klicken

Der Sendungstext:

Sehr geehrte Damen und Herren,

auch im Zuschauerkreis von Klagemauer-TV macht sich Unmut über arglistigen Betrug im Internethandel breit. So schrieb uns kürzlich Nicole aus Süddeutschland verzweifelt, dass sie unwissend in eine Internet-Falle getappt und ihre bestellte Spiegelreflexkamera bis heute noch nicht angekommen sei.

Doch was kann man gegen solch hinterlistige Betrügereien unternehmen? Wir von *Kla-TV* sind bestrebt, Ihnen mit unserem täglichen Sendungsangebot wiederkehrende Prinzipien und Handlungsmuster aufzuzeigen, die eine eigene und kritische Beurteilung der Ereignisse auf unserer Welt ermöglichen. In gleicher Weise möchten wir Ihnen heute anhand von praktischen Beispielen auch eine Hilfestellung bieten, die Sie bei der alltäglichen Internetnutzung vor irreparablen Schäden schützen kann.

Einige von Ihnen haben nachfolgende Situation vielleicht schon einmal erlebt:

- Sie öffnen ohne Böses zu ahnen Ihren E-Mail-Account, und dann schneit eine bedrohlich klingende Nachricht ins Postfach. Ups: Ihre Telefon-Rechnung vom vergangenen Monat sei noch nicht beglichen. Oder: Ihr Konto müsse aufgrund präventiver Sicherheitsvorkehrungen bis auf weiteres gesperrt werden. Ihr Adrenalin-spiegel schießt sogleich in die Höhe und Sie rücken mit weit aufgerissenen Augen und starkem Herzklopfen näher an den Bildschirm:
  - Sie werden aufgefordert, SOFORT zu handeln, indem Sie Daten angeben, ansonsten könne Ihr Konto unter der Kontrolle von Internet-

Betrügern bleiben oder jeden Moment der Gerichtsvollzieher vor der Tür stehen.

Doch aufgepasst!

Bei solchen E-Mails könnte es sich mit großer Wahrscheinlichkeit um *"Phishing"-E-Mails* handeln. "*Phishing*" meint nichts anderes, als dass jemand versucht, mittels üblen Tricks Ihre sensiblen Daten, wie z.B. Passwort und Benutzername, zu "*fischen*", um Sie hernach auf irgendeine Weise zu schädigen. Doch wie erkennt man, ob es sich bei einer elektronischen Nachricht um einen Betrugsversuch handelt oder nicht? Und was ist in einem solchen Fall zu tun? Um diese Fragen nicht nur in der Theorie zu beantworten, schalten wir nun zu unserem Computer-Experten nach Mannheim, der uns mit realen und erschreckenden Betrugsversuchen konfrontiert und uns Prinzipien im Umgang mit solchen Nachrichten vermittelt.

Besten Dank Studio Dresden für die verständliche Einleitung.

Meine Damen und Herren, schnallen Sie sich an - wir nehmen nun gemeinsam reale Phishing-E-Mails unter die Lupe und beurteilen diese anhand 4 Prüfungskriterien. Aufgepasst, genau diese und weitere durch Internet-Betrüger versandte E-Mails kursieren zurzeit im Internet und könnten auch Sie jeden Moment erreichen!

Wir haben hier nun unser Postfach geöffnet und rufen neue Nachrichten ab.

Tatsächlich es erreicht uns eine E-Mail mit dem Betreff "*Warnung Ihr PayPal-Konto wurde begrenzt“*.

1) Überstürzen Sie nichts! Lassen Sie sich zu keinen Panikhandlungen verleiten. Vergewissern Sie sich stattdessen in aller Ruhe zuerst, ob Sie überhaupt Kunde bei dem Gewerbe sind, das angeblich diese E-Mail versandt hat. Falls Sie eine E-Mail von einer Plattform erhalten, von der Sie noch nie etwas gehört haben oder bei der Sie kein Kunde sind, ist es äußerst unwahrscheinlich, dass eine Rechnung oder Mahnung berechtigt ist.
2) Verschaffen Sie sich einen Gesamteindruck durch die Prüfung der Rechtschreibung und des Absenders der E-Mail-Nachricht! Seriöse Firmen und Institutionen versenden keine elektronische Post mit einer irritierenden Absenderadresse oder mit auffallenden grammatikalischen Schreibfehlern.

Der erste Eindruck ist gut. Das Logo von PayPal kennen wir. Also lesen wir den Text:

- *"Sehr geehrter PayPal-Mitglied: Warnung! Ihr PayPal-Konto wurde begrenzt! Im Rahmen unserer Maßnahmen zur Gefahrenabwehr, gehen wir regelmäßig Screen Aktivitäten zu lernen PayPal vor kurzem kontaktiert Sie, nachdem sie identifiziert ein Problem auf Ihrem Konto. Um Ihre Karte zu reaktivieren herunterladen und füllen Sie das beigefügte Dokument. Diese Nachricht, damit wir den Fall zu lösen."*

BETRUG:

- Bei dieser Nachricht handelt es sich um einen unmissverständlichen Betrugsversuch. Seriöse Firmen und Institutionen versenden NIEMALS elektronische Post mit auffallenden grammatikalischen Schreibfehlern. Öffnen Sie auch auf keinen Fall Dateien, die der Nachricht angehängt sind. Bei den angehängten

Dateien handelt es sich mit großer Wahrscheinlichkeit um Viren, die Ihre Computer ausspionieren und sensible Daten an Internetbetrüger senden können. Löschen Sie die Nachricht aus dem Posteingang und anschließend auch aus dem Papierkorb Ihres E-Mail-Programms.

Wir rufen erneut unsere E-Mails ab und siehe da es erreicht uns eine Nachricht mit dem Betreff: *"Ihre Festnetz-Rechnung für Juli 2015".*

1) Vergewissern Sie sich, ob Sie Kunde bei dem Gewerbe sind, das angeblich diese E-Mail versandt hat!
2) Verschaffen Sie sich einen Gesamteindruck durch die Prüfung der Rechtschreibung und des Absenders der E-Mail-Nachricht!

Der erste Eindruck scheint zuverlässig. Es sind keine auffälligen Schreibfehler zu finden: *"Ihre Rechnung vom 12.7.2015 finden Sie im Anhang als PDF. Die Summe beträgt 160€ und ist am 22.07.2015 fällig"*.

Wir überprüfen die Absenderadresse und siehe da, die E-Mail wurde von einer Adresse aus versendet, die nichts mit Vodafone zu tun hat. Seriöse Firmen und Institutionen versenden keine elektronische Post mit einer irritierenden Absenderadresse.

3) Vergewissern Sie sich, dass sämtliche Internetlinks in der E-Mail auf die ORIGINALE Internetseite der Institution führen! Fahren Sie mit der Maus auf den Internetlink, der Sie zur Rechnung führt, die Sie angeblich zu begleichen haben. Klicken Sie NICHT darauf, sondern suchen Sie Auffälligkeiten im Internetlink. Der Internetlink würde uns auf eine Internetseite führen, die in keinster Weise etwas mit Vodafone zu tun hat!

BETRUG:

- Bezahlen Sie die Rechnung auf keinen Fall, sondern löschen Sie die Nachricht aus Ihrem Posteingang und anschließend auch aus dem Papierkorb Ihres E-Mail-Programms.

Wir rufen erneut unsere elektronische Post ab und *„Ach du Schreck“:* Scheinbar wurde Ihr Amazon-Konto wegen eines Betrugsversuchs gesperrt.

1) Überstürzen Sie nichts! Lassen Sie sich zu keinen Panikhandlungen verleiten!
2) Verschaffen Sie sich einen Gesamteindruck z. B durch die Prüfung der Rechtschreibung und des Absenders der E-Mail! "Bei der letzten Überprüfung Ihres Accounts sind uns ungewöhnliche Aktivitäten aufgefallen. Bitte bestätigen Sie Ihre hinterlegten Informationen, damit Sie ihren Account wieder in vollem Umfang nutzen können". Diese Information ist erschreckend und möchte Sie zu schnellem Handeln drängen! Diese Nachricht möchte uns weismachen, dass sich jemand Zugang zu unserem Amazon-Konto verschafft hat und ohne Ihr Geständnis eine Bestellung in Höhe von 590 € an einen gewissen Piotr Sobczak aus Hamburg versandt hat! Sowohl Rechtschreibung

wie Absenderadresse scheinen zu stimmen und nur ein Klick auf "Daten bestätigen" scheint Sie vor diesem Betrug noch retten zu können!

3) Vergewissern Sie sich, dass sämtliche Internetlinks in der E-Mail auf die ORIGINALE Internetseite der Institution führen! Internetbetrüger machen sich mit Vorliebe in diesem Punkt die Unwissenheit ihrer Opfer zunutze. Klicken Sie auf keinen Fall auf den Link. Denn wie uns schnell auffällt, würde uns dieser Link auf eine Adresse führen, die nichts mit Amazon zu tun hat. Lassen Sie sich nicht täuschen! Internetbetrüger bilden unter falschen Internetlinks komplette Internetseiten nach, die EXAKT gleich aussehen wie die originale Internetseite. Doch bei der Eingabe Ihrer persönlichen Daten werden Ihre Passwörter an die Betrüger versendet, die Sie hernach ungestört ausrauben können.

BETRUG:

4) Falls Sie sich dennoch vergewissern möchten, dass sich kein Betrüger Zugang zu Ihrem Konto verschafft hat, melden Sie sich UNABHÄNGIG von der E-Mail-Nachricht bei der Internetplattform mit Ihren Nutzerdaten an. Suchen Sie nach Ihrer Anmeldung im passwortgeschützten Bereich nach einem Hinweis, der die Warnung in der E-Mail bestätigt.

Für unser letztes Praxisbeispiel rufen wir erneut unsere E-Mails ab und erschrecken schon wieder beim Erhalt der Nachricht: "*PayPal- Nicht autorisierte Zahlung über 247 EUR"*.

1) Überstürzen Sie nichts! Lassen Sie sich zu keinen Panikhandlungen verleiten!
2) Verschaffen Sie sich einen Gesamteindruck z.B durch die Prüfung der Rechtschreibung und des Absenders der E-Mail! Der Gesamteindruck sieht sehr gut aus. Wir kennen den Absender und auch der Aufbau der E-Mail ist exakt gleich, wie die Nachrichten, die wir nach jedem elektronischen Einkauf mit PayPal erhalten: “Eine Prüfung der unten stehenden Transaktion hat ergeben, dass sie möglicherweise nicht durch Sie autorisiert wurde. Um weiteren Betrug zu verhindern, wurde Ihr PayPal-Konto bis auf weiteres eingeschränkt. Wir bitten Sie daher, Ihr PayPal-Konto mit nachfolgendem Link zu bestätigen, um die Einschränkung Ihres Kontos aufzuheben.“ Es ist erschreckend: Jemand scheint Ihre Zugangsdaten und somit Zugriff auf Ihr PayPal-Konto zu haben und damit eine Zahlung von über 247€ veranlasst zu haben! Doch Rettung scheint nahe: Durch einen Klick auf "Daten bestätigen" und die darauffolgende Eingabe Ihrer Zugangsdaten wird Ihnen Hilfe versprochen.
3) Vergewissern Sie sich, dass sämtliche Internetlinks in der E-Mail auf die ORIGINALE Internetseite der Institution führen! Internetbetrüger machen sich mit Vorliebe in diesem Punkt die Unwissenheit ihrer Opfer zunutze. Selbst die Internetlinks scheinen für einen Laien auf den ersten Blick korrekt. Nur ein geschultes Fachauge merkt, dass es sich bei diesem Link ebenfalls um einen Betrugsversuch handelt! Klicken Sie also auf keinen Fall und konsequent nie

auf den Link aus einer E-Mail, der Ihnen Rettung vor Betrug verspricht! Nie sind Sie dem wahren Betrug näher als dann: Sie würden nämlich zu einer exakt falsch nachgebildeten PayPal-Internetseite weitergeleitet werden, welche nach der Eingabe Ihres Passwortes Ihre persönlichen Logindaten an Betrüger sendet, die Ihr Konto plündern könnten.

BETRUG:

4) Falls Sie sich vergewissern möchten, dass sich kein Betrüger Zugang zu Ihrem Konto verschafft hat, melden Sie sich UNABHÄNGIG von der E-Mail-Nachricht bei der Internetplattform mit Ihren Nutzerdaten an. Suchen Sie nach Ihrer Anmeldung im passwortgeschützten Bereich nach einem Hinweis, der die Warnung in der E-Mail bestätigt. An dieser Stelle können leider noch unzählige weitere Beispiele angefügt werden. Wir hoffen, dass Ihnen unsere Praxisbeispiele geholfen haben, sich weiterhin geschützt und frei im Internet zu bewegen! Danke für Ihre Aufmerksamkeit und ich übergebe zurück ans Studio Dresden.

Echt erschreckende und hinterlistige Nachrichten, die hier im Internet kursieren...

Besten Dank, Studio Mannheim. Sehr geehrte Damen und Herren, wir leben in einer Zeit, in der vermehrt "Operationen unter falscher Flagge" durchgeführt werden, um ganz gezielt politische, wirtschaftliche und gesellschaftliche Absichten zu verfolgen. So ist damit zu rechnen, dass solche hinterlistigen E-Mails gezielt von speziell dafür angeheuerten Personenkreisen versandt werden, um einen Hilfeschrei im Volk zu erzeugen. Dieser vom drangsalierten Volk kommende Hilfeschrei liefert dann die Begründung dafür, die allgemeine Informationsfreiheit einzuschränken, indem strengere Daten-Kontrollen eingeführt und die Zensur des Internets vorangetrieben wird!
Wenn Sie Hinweise oder Informationen haben, von welchen Personengruppen solche Betrugs-Nachrichten versandt werden, dann reichen Sie diese noch heute noch als Klage auf unserer Internetseite ein.
Verbreiten Sie auch diese Sendung, damit auch Ihre Freunde, Bekannte und Verwandte nicht hinterlistigen Internetbetrügern auf den Leim gehen und das Internet auch in Zukunft frei und offen bleibt. Auf Wiedersehen.