Kennen Sie den Unterschied zwischen einer sicheren und einer betrügerischen E-Mail?

Kennen Sie den Unterschied zwischen einer sicheren und einer betrügerischen E-Mail?

In Sicherheitswissen by Jochen on April 30, 2015 | Français, English, Deutsch
Mehr als eine Milliarde Personen senden und empfangen täglich E-Mails. Davon werden jeden Tag 8.000 Personen von betrügerischen E-Mails heimgesucht, und insgesamt vier Millionen Personen werden jährlich Opfer von E-Mail-Betrügereien. Dabei ist es für jeden von grundlegender Bedeutung, eine sichere E-Mail von potenziellem Betrug unterscheiden zu können, da unbedachtes Öffnen von Anhängen und Nachrichten Sie schnell mit finanziellen Verlusten und Identitätsdiebstahl konfrontieren können.

45 % aller Nutzer fallen auf Betrugs-E-Mails herein und erleiden finanzielle Verluste oder Identitätsdiebstahl.

Laut Scamdex sind folgende die fünf häufigsten E-Mail-Betrügereien, vor denen Sie auf der Hut sein sollten:

#1) Arbeitsplatzangebote – gefälschte Jobangebote (Heimarbeit)

Mit diesen Mails werden Personen geködert, die Arbeit suchen oder ihre Arbeitsstelle wechseln möchten. Bei den meisten Jobangeboten handelt es sich im Internet um Heimarbeit, bei der große Geldsummen für wenig Arbeit versprochen werden. Viele derartige Angebote sind Scheckbetrügereien, bei denen Betrüger auf illegale Art und Weise Schecks eines Opfers zum Erwerb von Geldmitteln

nutzen, die nicht auf dem Konto so vorhanden sind. Diese Art von Betrugs-E-Mails können Sie daran erkennen, dass Bilder mit Geld oder Autos, Kundenaussagen, Zahlgebühren und großspurigem Text verwendet werden.

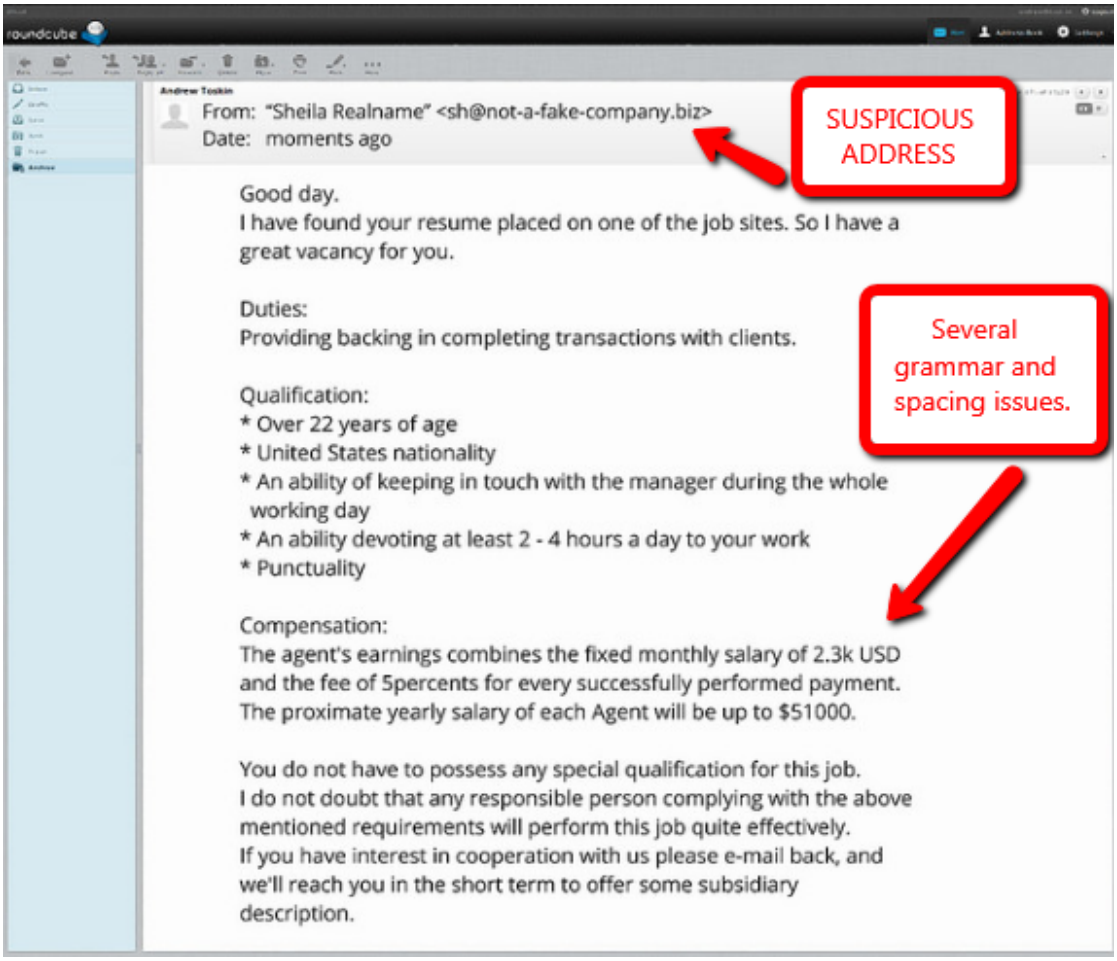

Foto von Andrew Toskin, Flickr

Bedenken Sie, dass die meisten Jobangebote für Heimarbeit oftmals zu schön, um wahr zu sein, sind. Lassen Sie Ihren gesunden Menschenverstand walten und seien Sie auf der Hut vor betrügerischen E-Mails, in denen Ihnen ein saftiges Gehalt für leichte oder wenig Arbeit angeboten wird. Geben Sie niemals persönliche Daten an Betrüger weiter, die Ihnen unaufgefordert Jobangebote per E-Mail zusenden. Antworten Sie nicht auf diese Nachrichten, sondern löschen Sie sie einfach direkt, bevor die Betrüger erst überhaupt an Ihre E-Mail-Adresse gelangen.

#2) Auktions-Betrugs-E-Mails – gefälschte Nachrichten von Shopping-Websites wie eBay und Amazon

Wir alle lieben Online-Shopping. Leider versuchen Betrüger so auch, Personen

hinters Licht zu führen, die sich nicht dessen bewusst sind, dass es sich um Betrug handelt. Augen auf bei Produkten, die Ihnen zu niedrigen Preisen angeboten werden, bei schlechten Bewertungen bei Auktionen, beim Abschluss einer Transaktion außerhalb einer Auktion und bei Verkäufern, die auf umgehende Zahlung beharren.

Betrüger geben vor, Ihnen ein Produkt zu einem sehr günstigen Preis zu verkaufen, um an Ihre Kreditkarten- und Bankdaten zu gelangen. Ein weiterer Trick von Betrügern besteht darin, bei Online-Auktionen ein niedriges Gebot abzugeben, dem dann ein hohes Gebot mit einem anderen Namen folgt, für ein Produkt, das Sie verkaufen möchten. Seien Sie ebenso gewarnt vor "Wunderprodukten" beim Online-Verkauf, die augenscheinlich unglaubliche Heilung oder Gewichtsverlust versprechen.

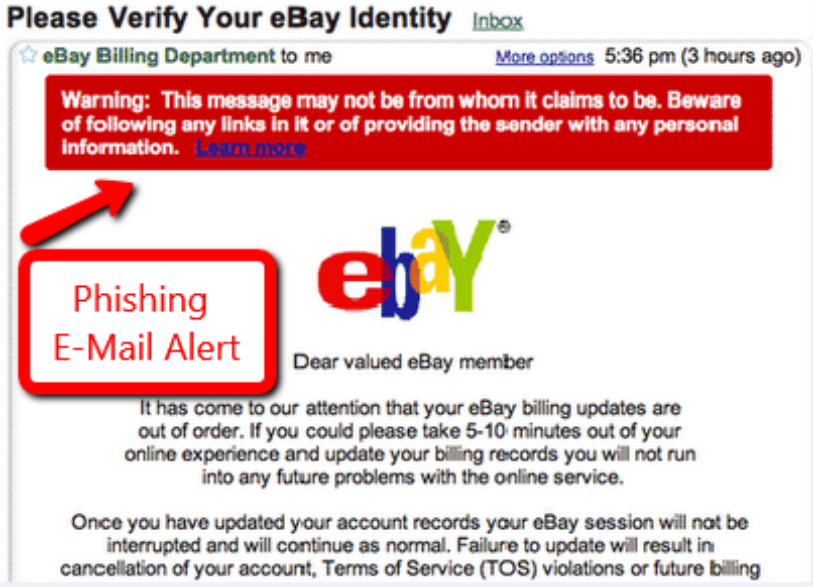

Foto von Jett, Bet You Didn't Know Blogspot

Bringen Sie immer genau in Erfahrung, mit wem und womit Sie bei Online-Auktionen zu tun haben, und sorgen Sie für sichere Zahlung durch eine verschlüsselte Verbindung (https://). Auch sollten Sie einen Blick in die Bestimmungen zum Datenschutz sowie zur Erstattung und Rückgabe werfen, damit alles mit rechten Dingen zugeht.

#3) Phishing-Betrugs-E-Mails – gefälschte Nachrichten von Paypal, dem Sozialamt oder Banken

Von dem **1%** der Nutzer, die durch Phishing Geld verloren haben, wurden **53%**

nicht von ihrer Bank abgefunden, und **11%** warten nach eigener Aussage noch auf ihre Erstattung. Laut einer Studie von Googleüber Phishing-Angriffe:

> *"Die meisten von uns denken, dass wir zu schlau, um auf Phishing hereinzufallen, aber unsere Studie ein paar gefälschte Websites aufgetan, die bei unglaublichen **45 %** der Fälle zum Erfolg führten."*

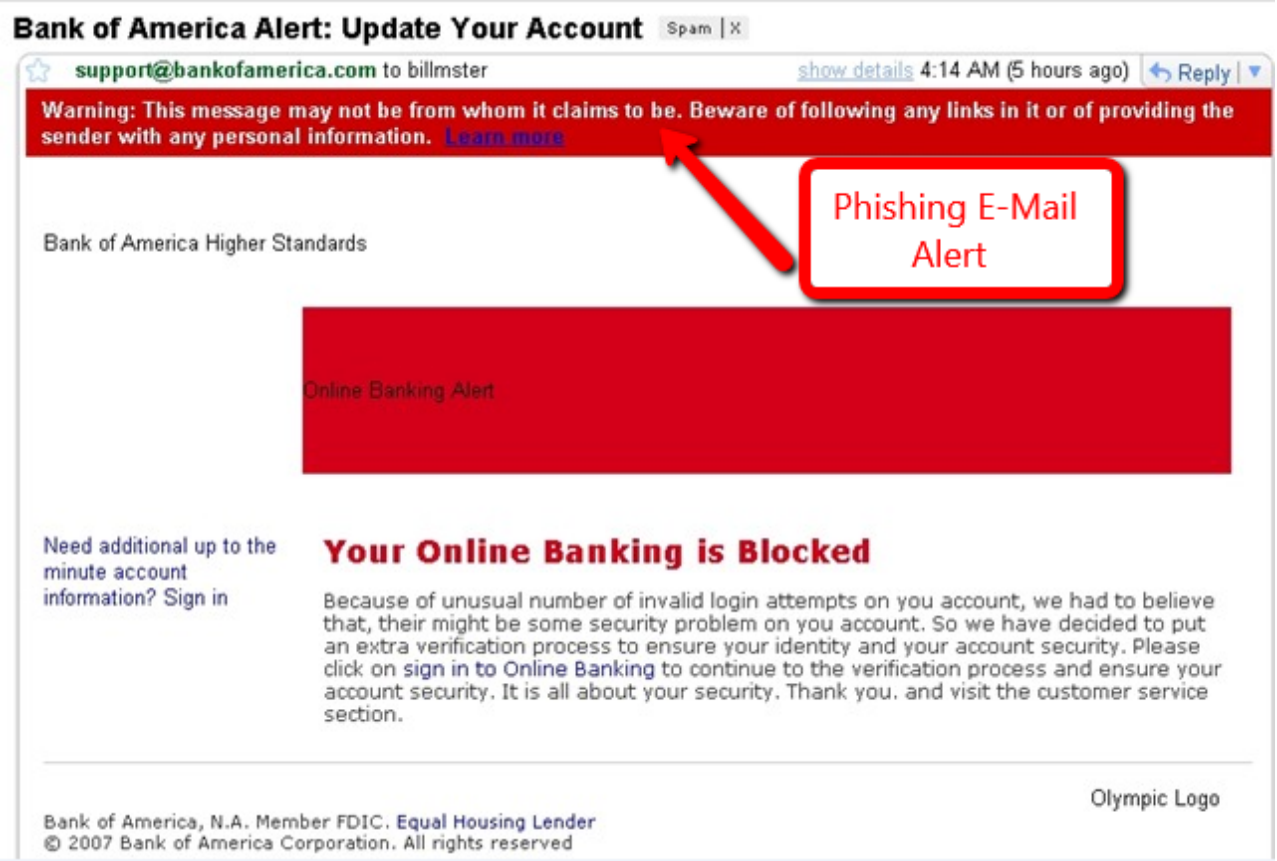

Foto von Quintana Hanson, Tax Refund

> *Phishing-E-Mails sehen oftmals **offiziellen Nachrichten von Verkäufern**, Facebook, Banken, Paypal und eBay täuschend ähnlich. In den Nachrichten werden Sie oft zur Bestätigung von Angaben und zur unmittelbaren Ausführung von Aktionen rund um Ihr Konto gebeten, wie z. B. der Bestätigung Ihrer Kontodaten. Die meisten Phishing-E-Mails enthalten besondere Links, die Sie zu echten und gefälschten Websites führen. Fallen Sie nicht auf die Unmenge an Liefer- und Paketverfolgungs-Betrugs-E-Mails herein, laut derer ein Paket mit einem beliebten Versanddienst wie Fedex oder UPS auf dem Weg zu Ihnen sein soll.*

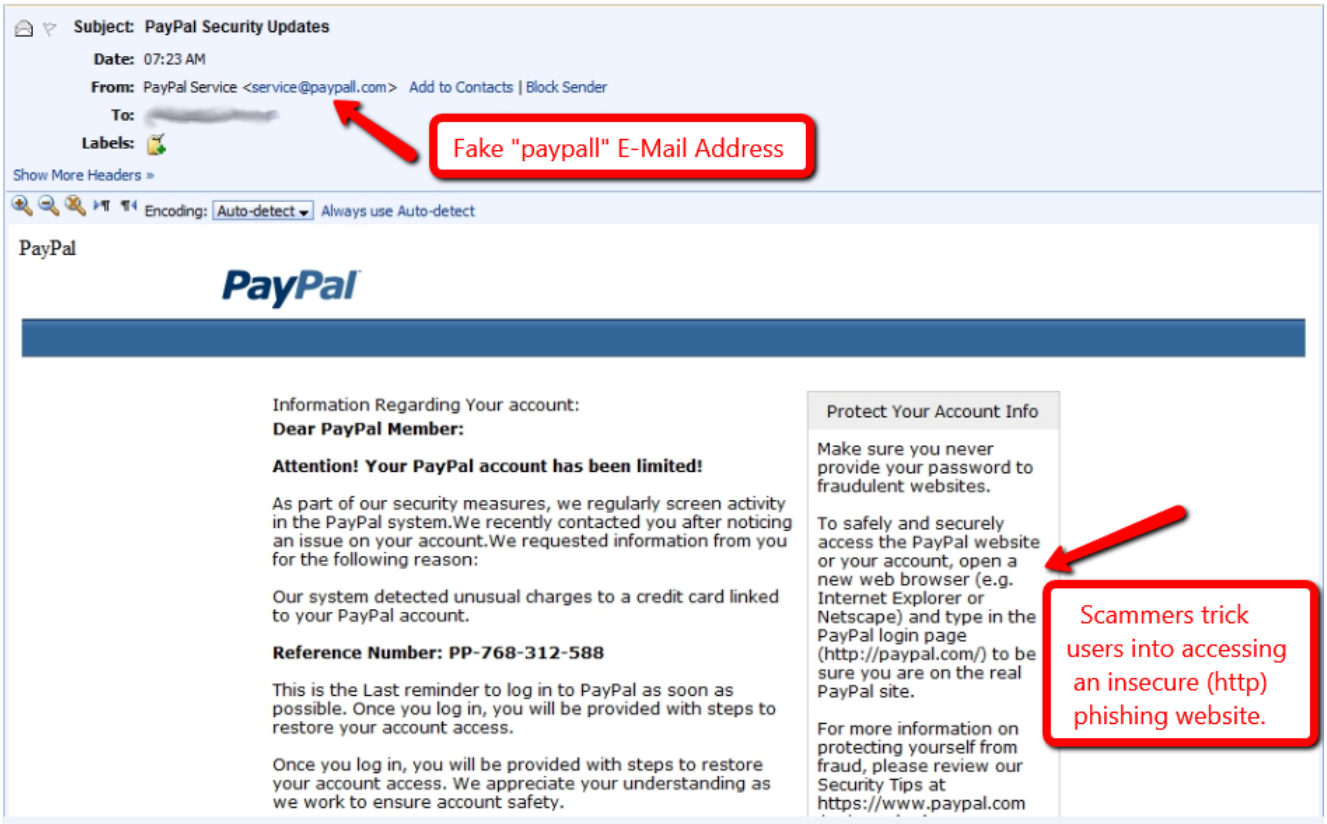

Foto von Saidul A Shaari, Flickr

Damit Sie diesen Betrügern nicht zum Opfer fallen, sollten Sie niemals Geld oder persönliche Daten an Fremde senden. Überprüfen Sie regelmäßig Ihre Kreditkartenabrechnungen und Kontoauszüge und vernichten Sie alle wichtigen Dokumente, die persönliche Daten enthalten. Melden Sie sich stets direkt auf Websites an und klicken Sie nicht auf verdächtige Links in E-Mails.

Google fand ebenfalls heraus, dass Nutzer oftmals wenig Zeit zur Wiederherstellung oder Änderung ihrer Anmeldedaten haben, bevor Hacker bereits Zugriff auf ihr Konto haben.

> *"Etwa **20%** der abgegriffenen Konten sind innerhalb von **30 Minuten** geknackt, nachdem ein Hacker die Anmeldedaten hat."*

#4) Lotterie- und Geschenk-Scams – ausländische Lotterien, Gewinnspiele und kostenfreie Urlaubsgeschenke

Lotterie- und Gewinnspielbetrügereien versprechen dem Empfänger tolle Preise. Diese Art von Betrugs-E-Mails treten in einer Vielzahl von Formen auf – per Telefon, persönlich, per E-Mail oder per Post. Die Betrüger geben vor, Sie hätten

eine beträchtliche Geldsumme gewonnen und müssten lediglich den Preis reklamieren, indem Sie Geld in Form von Gebühren wie Steuern, Zoll, Versand usw. zahlen. Üblicherweise bitten Nutzer darum, die Gebühren vom Gewinn abzuziehen, doch immer erhalten sie die gleiche Antwort von den Betrügern: “Das können wir leider nicht machen.”

Foto von Jamil Velji, Wikipedia

Seien Sie vorsichtig bei Urlaubs-Betrugs-E-Mails, bei denen Ihnen ein kostenloser Urlaub versprochen wird, Sie aber eine angebliche Servicegebühr zahlen oder eine Mitgliedschaft in einem Reiseclub erwerben müssen. Konsultieren Sie stets einen Finanz- oder Rechtsexperten, bevor Sie Geld senden.

#5) Betrugs-E-Mails mit Zusatzgebühren – Versprechen von Geld, Produkten, Dienstleistungen und Sonderangeboten

Betrug mit Zusatzgebühren ist eine beliebte Masche bei Betrugs-E-Mails, die auch als Vorausgebührbetrug bekannt ist. Dabei handelt es sich um Betrugs-E-Mails, bei denen Ihnen Gebühren berechnet werden und im Gegenzug Geld, Produkte, Dienstleistungen und Sonderangebote versprochen werden. Darüber hinaus werden Sie eventuell auch darum gebeten, Geldmittel aus einem Land in Aufruhr zu schaffen oder Strafverfolgungsbehörden beim Ergreifen von Dieben zu helfen.

Die bekannteste Betrugsmasche dieser Art mit einer Vielzahl von betroffenen Nutzern ist der sog. “419 Nigerian Scam”. Dabei wenden sich Betrüger üblicherweise an Sie per Post oder E-Mail und bieten einen Anteil einer großen Geldsumme, die sie außer Landes schaffen möchten. Der Empfänger wird dann zur Zahlung eines Betrags oder Preisgabe seiner Kontodaten gebeten, um beim Transfer behilflich zu sein. Das Opfer muss Gebühren, Kosten und Steuern zahlen, damit das Geld außer Landes geschafft werden kann. Die Betrüger erfinden dann weiterhin Gebühren, die Sie zahlen müssen, bevor Sie Ihr Geld erhalten.

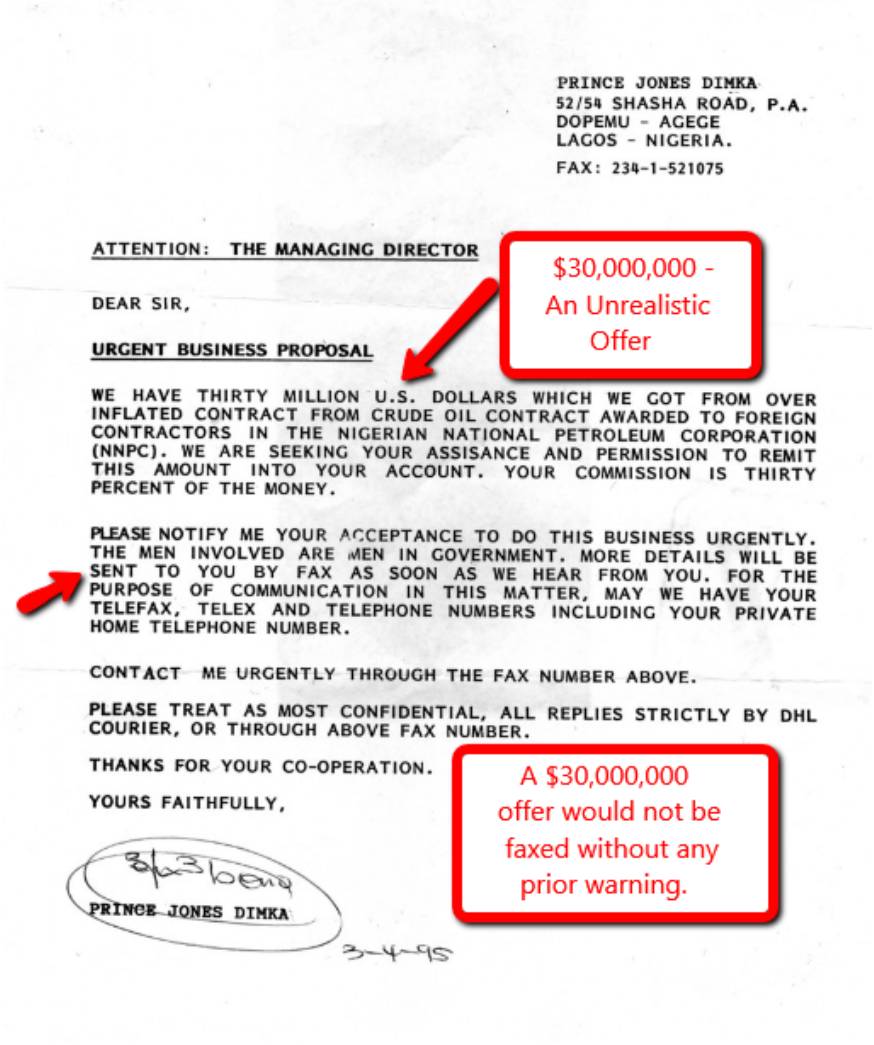

Bild von Morburre, Wikipedia

Natürlich erhalten Sie niemals das versprochene Geld. Laut der Website von Nigerian Fraud Watch wurden die Opfer dabei um atemberaubende **12,7 Milliarden Dollar** gebracht.

Nutzer nehmen E-Mails so wahr, wie sie auf den ersten Blick erscheinen

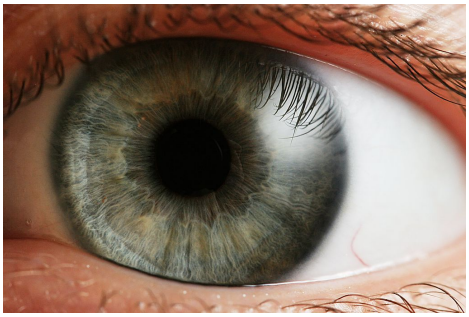

Foto von Petr Novák, Wikipedia

Vier beliebte Universitäten – die University of Buffalo, Brock University, Ball State University und die University of Texas in Arlington – haben eine Studie und gegen eine Gruppe von Nutzern einen Phishing-Angriff ausgeführt. Die Absicht dahinter war es, die psychologischen Gründe dafür zu eruieren, warum Menschen auf Phishing-E-Mails hereinfallen. So heißt es:

> *"Unsere Ergebnisse lassen erkennen, dass Menschen die meisten Phishing-E-Mails nur am Rande wahrnehmen und* ***ihre Entscheidung basierend auf einfachen Hinweisen in der E-Mail treffen****. Interessanterweise führten dringliche Hinweise wie Bedrohungen oder Warnhinweise zu erhöhter Informationsverarbeitung, was Ressourcen zur Beachtung anderer Hinweise abzieht und so potenziell die Erkennung des Betrugs verhindert."*

Bei der Studie kann man zu ein paar Schlüssen:

1. Die Nutzer verarbeiten nur, was mit eigenen Augen sehen, und achten nicht auf den potenziellen Betrug, den sie im Hinterkopf haben.
2. Sie treffen Entscheidungen, eine E-Mail zu öffnen und zu lesen, basierend auf auffälligen Titeln, Grafiken, Aussagen und Dringlichkeitshinweisen wie "Ihr Bankkonto wird gesperrt, wenn Sie nicht jetzt reagieren". Das Angstmoment spielt ebenso eine Rolle, da ein Nutzer sich oft vom Titel oder einem Teil einer E-Mail abschrecken lässt, ohne sich auch nur fragen, ob das sein kann oder warum.
3. Dringlichkeitshinweise in einer E-Mail führen zu einer Informationsüberflutung. Oftmals findet sich zu viel Inhalt in einer E-Mail,

was dazu führt, dass unser Gehirn zu viel auf einmal verarbeiten muss und so einer Reizüberflutung erliegt. Einprägsame Titel und auffällige Inhalte/Grafiken führen oft dazu, dass Nutzer Warnhinweise ihrer Sicherheitssoftware oder Warnmeldungen ihres E-Mail-Filters übersehen, die Sie zur Vorsicht aufrufen und so den Betrug als solchen erkennen könnten, bevor sie ihm zum Opfer fallen.

"Unsere Ergebnisse legen nahe, dass ***Verhaltensmuster in der Mediennutzung in Verbindung mit einer großen Zahl an E-Mails*** *einen deutlichen Einfluss auf die Wahrscheinlichkeit jedes Einzelnen haben, Phishing zum Opfer zu fallen."*

So gehen Sie E-Mail-Betrügereien aus dem Weg

- Achten Sie auf unaufgefordert zugesandte E-Mail-Anhänge von verdächtigen E-Mail-Adressen. Klicken Sie niemals auf augenscheinlich verdächtig aussehende Links. Fahren Sie mit der Maus über einen Link, um die Zieladresse anzuzeigen und zu erkennen, ob es sich hierbei um keinen Betrug handelt.
- Klicken Sie auf keine Links in E-Mails, bei denen Sie zur Anmeldung mit einem Passwort aufgefordert werden. Besuchen Sie stattdessen lieber selbst die Website, melden sich an und suchen nach den Informationen, die in der E-Mail beworben werden.
- Fallen Sie nicht auf fünf beliebtesten E-Mail-Betreffzeilen herein, die Betrüger verwenden: Einladungen zur Kontaktaufnahme auf LinkedIn, "Mail delivery failed: returning message to sender", Lieber (Name) Kunde, Comunicazione importante und "undelivered mail returned to sender".
- Verwenden Sie einen Spam-/Junkmail-Filter. Lernen Sie, Ihre E-Mails zu filtern, um so die Spreu vom Weizen zu trennen. Laut Kaspersky sind mehr als 70 % der E-Mails Spam. Eine andere Möglichkeit besteht in der Verwendung einer speziellen Software zur Filterung und Blockierung potenziell unsicherer Nachrichten wie MailWasher.

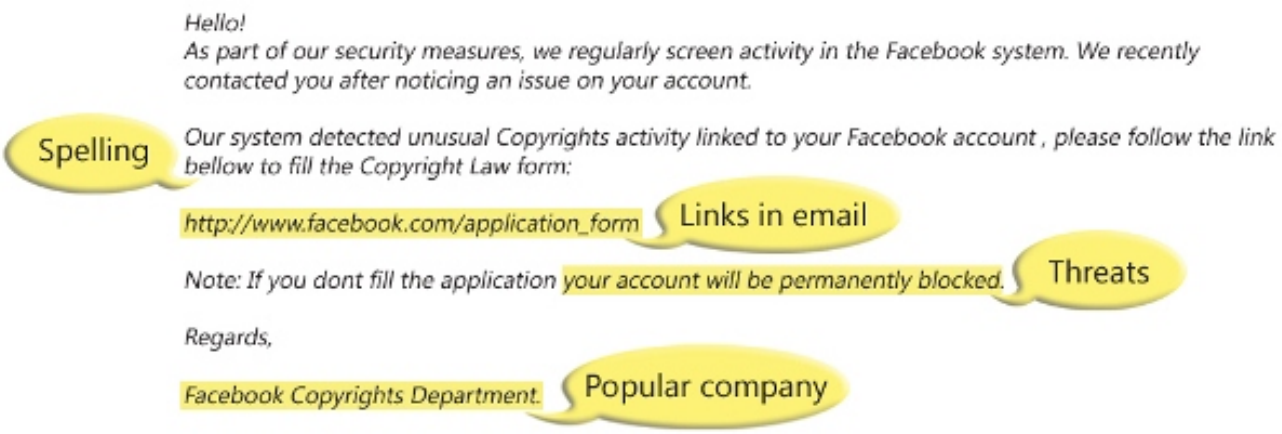

Foto und Inhalte von Microsoft

- Erscheint eine E-Mail Ihnen augenscheinlich verdächtig, stellen Sie über andere Wege Kontakt her und überprüfen Sie die Herkunft und Authentizität der E-Mail. Sollte es sich um eine legitime E-Mail handeln, so sollte es ein Leichtes sein, eine Telefonnummer herauszufinden.

Haben Sie diese Arten von E-Mail-Betrügereien gesehen? Welche anderen kennen Sie?

Wir wünschen eine schöne (Spam-freie) Zeit!