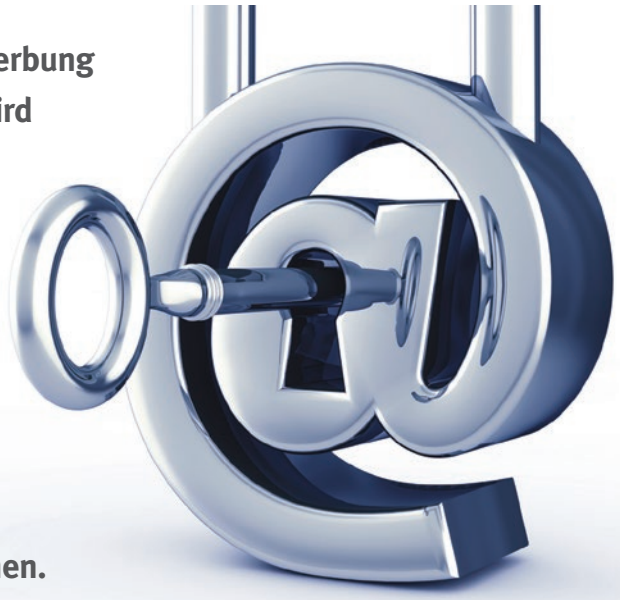
Die Verbraucherzentrale NRW gibt Tipps:

Vorsicht vor betrügerischen E-Mails



Nicht nur der heimische Briefkasten ist oft mit Werbung verstopft, auch der elektronische Briefkasten wird immer mehr zugemüllt. Während Sie Werbung im heimischen Briefkasten alternativ zur direkten Entsorgung in der Regel gefahrlos öffnen können, müssen Sie in der digitalen Welt die nötige Portion Misstrauen an den Tag legen, um Gefahren vorzubeugen. Eine dieser Gefahren heißt Phishing. Dr. Annabel Oelmann von der Verbraucherzentrale NRW erläutert, was Phishing ist und wie sich Verbraucher vor den Gefahren schützen können.

aktiv: Frau Oelmann, fangen wir mit der grundsätzlichen Frage an: Was ist Phishing eigentlich?

Dr. Annabel Oelmann: Phishing setzt sich aus dem englischen Begriff für Passwort-Fischen zusammen. Das Bundesamt für Sicherheit in der Informationstechnik erläutert den Begriff wie folgt: „Phishing ist ein Kunstwort aus "Passwort" und "Fishing" und bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden. Hierzu werden häufig Methoden des Social Engineering, teilweise in Verbindung mit Identitätsdiebstahl, verwendet. Beispielsweise können die Angreifer geschickt formulierte E-Mails an die Benutzer senden."

Den Kriminellen geht es also darum, Sie dazu zu bringen, persönliche Daten wie beispielsweise PIN, Girokontonummer oder Kreditkartennummer preiszugeben. Die Phishing-E-Mail ist so konstruiert, dass sie Vertrauen schafft und den Eindruck erweckt, von einem echten Anbieter zu stammen. Kriminelle geben sich also als Absender eines tatsächlich existierenden Unternehmens aus – beispielsweise Bank, Kreditkartenunternehmen oder Zahlungsdienstleister – und versuchen, Sie zur Eingabe von persönlichen Daten zu bewegen. In der Regel geschieht dies über einen in der E-Mail hinterlegten Link, der Sie zu einer nachgebauten Internetseite des in der E-Mail genannten Unternehmens führt. Alternativ versuchen die Kriminellen, Sie dazu zu bewegen, einen Datei-Anhang zu öffnen. Dieser enthält ein trojanisches Pferd – umgangssprachlich besser bekannt als Trojaner – und soll ihren Computer ausspionieren.

aktiv: Wie ist sieht eine Phishing-E-Mail aus?

Dr. Annabel Oelmann: Jeden Tag werden viele unterschiedliche Varianten von Phishing-E-Mails versendet. Auch wenn diese in äußerer Form und inhaltlichem Text verschieden sind, gibt es doch übereinstimmende Merkmale im Aufbau der Mail:

- Die Anrede: Bei vielen Phishing-Mails steht eine allgemeine Anrede wie „Liebe Kunden" oder „Sehr geehrte Damen und Herren". Leider ist umgekehrt eine persönliche Anrede kei-

Foto: nobeastsofierce/Fotolia.com

ne Garantie, dass die E-Mail echt ist, sondern nur ein Indiz, dass sie möglicherweise echt sein könnte. Denn immer häufiger werden die E-Mail-Empfänger in Phishing-Mails auch persönlich mit Vor- und Zunamen angesprochen.

- Der Grund der E-Mail: Nach der Anrede erfährt der E-Mail-Empfänger, warum diese Mail verschickt wird. Hier verfügen die Kriminellen über einen bunten Strauß an erfundenen Gründen. Beliebt sind zum Beispiel Gesetzesänderungen, die Einführung einer neuen Sicherheitstechnik oder Unstimmigkeiten im Kundenkonto, die geklärt werden müssen.

- Die Notwendigkeit zum Handeln: Nachdem der Grund für die Versendung der E-Mail erklärt wurde, geht es jetzt darum, dass der E-Mail-Empfänger aktiv werden muss. In der Regel soll er seine Daten erneut eingeben, kontrollieren, bestätigen oder verifizieren.

- Der Zeitdruck: Damit die E-Mail-Empfänger nicht zu lange nachdenken können und am Ende doch noch misstrauisch werden, gibt es oft nur eine kurze Zeitspanne für das vermeintlich notwendige Handeln. Dies können beispielsweise 48 Stunden, sieben Tage oder das Ende des laufenden Monats sein.

- Die Konsequenzen des Nichthandelns: Wer nicht innerhalb dieser kurzen Frist aktiv wird, dem werden schwere Konsequenzen angedroht. Oft geht es darum, dass ein Kontodienst eingeschränkt wird, gar nicht mehr genutzt werden kann oder sogar aufgelöst wird.

- Link oder Anhang: Die Kriminellen fügen der E-Mail einen Link oder einen Datei-Anhang bei. In wenigen Ausnahmefällen geht es darum, dass eine Antwort per E-Mail erbeten wird. Der angebotene Weg, entweder auf den Link zu klicken oder den Anhang zu öffnen, wird als einfache und kostenlose Lösung, als zwingend notwendig oder als Service verkauft.

aktiv: Wie schütze ich mich vor einer Phishing-E-Mail?

Dr. Annabel Oelmann: Die drei wichtigsten Regeln im Umgang mit unerwarteten E-Mails lauten:

1. Klicken Sie niemals auf Links
2. Öffnen Sie niemals Datei-Anhänge
3. Antworten Sie nicht auf diese E-Mails

Wenn Sie diese drei Regeln beherzigen, haben Sie die größte Gefahrenquelle im Umgang mit unerwarteten E-Mails schon ausgeschaltet. Haben Sie eine E-Mail als Betrugsversuch entlarvt, löschen Sie diese. Aber bitte leiten Sie die E-Mail vor dem Löschen an phishing@vz-nrw.de weiter. Denken Sie an Ihre Mitmenschen, die solche E-Mails nicht als Betrug erkennen. Mit der Weiterleitung helfen

Foto: weerapat1003/Fotolia.com

Sie uns, andere Menschen vor solchen kriminellen Machenschaften zu warnen.

Es gibt eine ganze Reihe weiterer Maßnahmen, die Sie treffen können, um das Risiko zu minimieren, Opfer von Kriminellen zu werden (s. Kasten).

aktiv: Was mache ich, wenn ich unsicher bin, ob die E-Mail nicht doch echt ist?

Dr. Annabel Oelmann: Inzwischen sind viele Phishing-E-Mails leider so gut gemacht, dass man sie nicht mehr an Tippfehlern oder ungewöhnlichen Wortstellungen erkennen kann. Daher sind viele Verbraucher durchaus verunsichert, wenn sie eine unerwartete E-Mail in perfektem Deutsch bekommen. Niemand möchte auf eine Phishing-E-Mail hereinfallen, gleichzeitig will aber auch niemand eine echte E-Mail ignorieren.

Jetzt ist es entscheidend, nicht vorschnell zu handeln. Denn genau darauf setzen die Kriminellen – dass Sie im ersten Schreck den Anhang öffnen oder auf einer präparierten Seite Daten eingeben. Das wäre aber der größte Fehler, den Sie an der Stelle überhaupt machen können.

Sind Sie – was vorkommen kann – tatsächlich Kunde des in der E-Mail genannten Unternehmens und wollen sich vergewissern, ob der Inhalt nicht doch

Was kann ich sonst noch tun?

1. Halten Sie das Virenschutzprogramm, den Internetbrowser und das Betriebssystem stets auf dem aktuellen Stand.
2. Eine Firewall hilft, unerlaubte Netzwerkzugriffe zu unterbinden.
3. Geben Sie die Internetadresse zu Ihrer Bank immer selbst per Hand in den Browser ein.
4. Gehen Sie mit persönlichen Daten im Internet sehr sparsam um. Je freigiebiger Sie diese preisgeben, um so größer ist die Gefahr, dass Ihre Daten in einen Verteiler geraten, den Kriminelle nutzen.
5. Verwenden Sie mehrere E-Mail-Adressen, damit nicht alle Bereiche Ihres Lebens betroffen sind, falls doch einmal eine Ihrer E-Mail-Adressen in einen Verteiler gerät, den Kriminelle nutzen. Idealerweise nutzen Sie für das Online-Banking eine separate E-Mail-Adresse, die nur Ihre Bank kennt.
6. Sichern Sie wichtige Daten auf einer externen Festplatte statt auf dem Computer.
7. Ändern Sie in regelmäßigen Abständen Passwörter und Sicherheitsfragen. Achten Sie darauf, dass Ihr Passwort aus wenigstens zehn Zeichen besteht, die Großbuchstaben, Kleinbuchstaben, Zahlen und mindestens ein Sonderzeichen beinhalten, so dass Dritte dieses nicht erraten können.
8. Kontrollieren Sie regelmäßig Ihre Kontoauszüge.

Foto: goodluz/Fotolia.com

echt ist, dann spricht grundsätzlich nichts dagegen, den echten Anbieter zu kontaktieren. Aber tun Sie das keinesfalls, indem Sie auf die E-Mail antworten oder eine in der E-Mail genannte Kontaktmöglichkeit nutzen. Wenn möglich, gehen Sie in eine Filiale des Anbieters und fragen Sie dort nach. Ist das nicht möglich, finden Sie eine Kontaktmöglichkeit auf der echten Internetseite des Anbieters.

aktiv: Was soll ich tun, wenn ich doch mal auf die Kriminellen reingefallen bin?

Dr. Annabel Oelmann: Wenn Sie auf Kriminelle reingefallen sind, müssen Sie, um (weiteren) Schaden zu vermeiden, folgende zwei Dinge beachten: Handeln Sie schnell und zeigen Sie keine falsche Scham. Sie sind nicht der Erste, der auf solch einen miesen Trick hereingefallen ist und Sie werden auch nicht der Letzte sein. Konkret sollten Sie folgendes tun:

- Sperren Sie sofort die betroffenen Konten und Karten. Kontaktieren Sie daher als allererstes Ihre(n) Anbieter.
- Stellen Sie Strafanzeige bei der Polizei. Die Phishing-E-Mail dürfen Sie im Nachhinein nicht mehr löschen, da diese jetzt ein wichtiges Beweismittel ist.
- Kontrollieren Sie, ob sich auf ihren Computern und/oder ihren mobilen Geräten ein Virus oder ein trojanisches Pferd befindet. Nutzen Sie die befallenen Geräte nicht, bevor dieser wieder sicher sind.
- Ändern Sie mit einem nicht befallenen Gerät Passwörter und Sicherheitsfragen. Achten Sie darauf, dass Ihr Passwort aus wenigstens zehn Zeichen besteht, die Großbuchstaben, Kleinbuchstaben, Zahlen und mindestens ein Sonderzeichen beinhalten, sodass Dritte dieses nicht erraten können.

Unter der Adresse www.vz-nrw.de/phishing finden Internetnutzer das Phishing-Radar der Verbraucherzentrale. Dort gibt es weitergehende Informationen zum Thema Phishing und Hinweise zu aktuellen Betrugswellen.

So könnte eine Phishing-Mail aussehen:

PayPal

Auffällige Transaktion festgestellt - Bestätigung erforderlich!

Sehr geehrte(r) Kunde(in),

bei Ihrer letzten Zahlung haben wir Auffälligkeiten festgestellt.

Ihr letzter Einkauf in Höhe von **379,00 €** bei dem Online-Shop ***Christ*** wurde zu Gunsten Ihrer Sicherheit vorerst nicht genehmigt. Hierüber gelangen Sie zum jeweiligen Produkt.

Wir haben festgestellt, dass Sie sich von einem uns nicht bekannten Gerät angemeldet und diese Zahlung durchgeführt haben.

Wenn Sie diesen Einkauf **nicht** getätigt haben, bitten wir Sie über den unten ausgeführten Button Ihre Daten zu bestätigen und anschließend die Bestellung zu stornieren.

Für die Stornierung der Bestellung haben Sie eine Frist von **14 Werktagen**. Läuft diese ab und Sie beantragen keine Stornierung, wird die Zahlung automatisch genehmigt.

Weiter zur Stornierung (hier klicken)

Wir bedanken uns bei Ihnen für Ihr Verständnis.

Mit freundlichen Grüßen

Ihr PayPal-Team