DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Schutz vor Phishing

Phishing-Seiten sprießen wie Pilze aus dem Boden. Derartige Internetseiten werden von Jahr zu Jahr authentischer, so dass man den Unterschied zur Original-Website kaum noch erkennen kann. So berauben Online-Kriminelle ihre oft ahnungslosen Opfer um deren Zugangsdaten mit dem Ziel, ihre Bankkonten leer zu räumen. Aber was bedeutet Phishing? Wie schütze ich mich vor derartigen Angriffen? Wie erkenne ich, dass ich einem Phishing-Angriff bzw. Versuch zum Opfer fiel? Was kann ich tun, wenn ich Opfer eines Phishing-Angriffs wurde?

Was bedeutet Phishing?
Beim Phishing (engl. angeln) nutzen Online-Kriminelle täuschend echte Köder wie Homepages von Banken, um Ihren Opfern persönliche Zugangsdaten wie Passwörter oder PINs Ihres Online-Banking-Zugangs zu entlocken. Geködert wird das Opfer meist mit E-Mails, die so echt wirken, dass man nur schwer einen Unterschied zur originalen Webseite bemerkt. Darin wird der Kunde aufgefordert, seine vertraulichen Daten einzugeben. Sind die Daten vom ahnungslosen Opfer einmal eingegeben, verschaffen sich die Täter Zugang zum Benutzerkonto des Phishing-Opfers und richten hohe finanzielle Schäden an. Als Köder werden bevorzugt Online-Anbieter genutzt, bei denen die Eingabe von Zugangsdaten notwendig ist. Zum Beispiel Online-Bankkonten, Online-Bezahlsystemen (wie PayPal) oder Online-Shopping-Anbieter (wie Amazon).

Wie kann ich mich schützen?
Zu aller erst kann eine gesunde Portion Misstrauen als Schutz gegen Phishing-Attacken hilfreich sein. Eine Bank verlangt niemals von Ihnen die Eingabe von Passwörtern oder TAN-Nummern via E-Mail. Bei offiziellen Anschreiben beginnt die Mail zudem meist mit einer direkten Anrede und nicht mit Formulierungen wie "Sehr geehrter Kunde". Das kann ein Zeichen für eine Phishing-Mail sein. Generell gilt: Wenn Sie unsicher sind, ob eine Mail echt ist, fragen Sie direkt bei dem Unternehmen nach.

Weitere Maßnahmen können Sie vor einem Phishing-Angriff schützen:

- **Browser-Nutzung**
  Im Zweifelsfall sollten Sie die Web-Adresse des gewünschten Unternehmens selbst im Internet-Browser eintippen oder ein gespeichertes Lesezeichen nutzen. Weiterhin verfügt jeder neuere Browser heutzutage über einen Phishing-Schutz bzw. einen Filter. Ist eine Webseite nicht vertrauenswürdig, wird diese vom Browser blockiert und der Nutzer darüber informiert.
- **Sichere Passwörter**
  Verwenden Sie für sensible Zugänge unbedingt sichere Passwörter. Wie Sie ein sicheres Passwort erstellen, erfahren Sie in unserem Ratgeber zum Thema "Sichere Passwörter".
- **HTML-Scripts deaktivieren**
  Deaktivieren Sie die HTML-Script-Funktion in Ihrem E-Mail-Programm. Denn die meisten Phishing-Mails greifen auf HTML-Scripts zurück. Sie können die Funktion wieder aktivieren, wenn Sie zum Beispiel eine E-Mail-Grußkarte anschauen wollen. Oder Sie nutzen einen E-Mail-Filter, wie ihn viele Antivirenprogramme bieten. Wichtig ist hier jedoch, dass Sie die Virenschutzsoftware regelmäßig aktualisieren.
- **Aktuelle Technologie für Online-Banking nutzen**
  Einige Kreditinstitute nutzen Zertifikate, um die Authentizität von Informationen zu

bestätigen. Andere Unternehmen bieten Chipkartenlesegeräte für die heimische Nutzung an. Wickeln Sie Ihr Online-Banking sicherheitshalber, anstatt über den Browser, über eine eigene Software ab.
Das Sicherheitspaket Komplett bietet zusätzlich eine Identity Safe-Funktion. Damit werden Ihre Anmeldedaten, Passwörter, persönlichen Daten und Ihre Identität beim Einkaufen im Web optimal geschützt.

- **Sichere E-Mail-Adresse**
  Die meisten Anbieter von E-Mail-Adressen sind heutzutage mit einem Spamschutz ausgerüstet. Nutzen Sie zum Beispiel E-Mail@magenta.de (Mail M), so erhalten Sie Spamschutz Plus inklusive für Ihr E-Mail-Konto und Ihr Postfach ist vor gefährlichen E-Mails geschützt.

Wie erkenne ich, dass ich einem Phishing-Angriff bzw. Versuch zum Opfer fiel?

E-Mails mit folgenden Inhalten können auf einen vermutlichen Phishing-Angriff hinweisen:

- Sie erhalten eine Warnung und Drohungen bezüglich einer Kontoschließung z. B. für Ihr Bankkonto oder ein Konto bei einem Online-Shopping-Anbieter wie Amazon. Es handelt sich hier meist um Unternehmen, mit denen Sie regelmäßig Geschäfte tätigen.
- Versprechungen von Geld für wenig oder keinen Aufwand, zum Beispiel durch Heimarbeit.
- Geschäfte, die sich zu gut anhören, um wahr zu sein.
- Aufforderung zu einer Spende an eine Wohltätigkeitsorganisation nach einer Katastrophe, die vor Kurzem in den Nachrichten war.

Weitere Anzeichen sind:

- Grammatik- oder Schreibfehler in der empfangenen E-Mail oder im integrierten Ziel-Link können auf eine gefälschte Website führen, wo Sie zur Eingabe persönlicher Informationen aufgefordert werden. Oder Phishing-Mails können so aussehen, als ob Sie von jemandem aus Ihrem E-Mail-Adressbuch gesendet wurden. Achten Sie auf Schreibfehler in E-Mail-Adressen oder Ziel-Links wie Mirosoft (anstatt Microsoft), ebay.de.z009.com oder visacrad.com.
- Einige Phishing-E-Mails können original aussehende Logos und andere Informationen von seriösen Websites beinhalten oder überzeugende Details über Ihre Vergangenheit beinhalten, die Betrüger in sozialen Netzwerken über Sie gefunden haben.
- Sie können in Phishing-Mails aufgefordert werden, eine Telefonnummer anzurufen. Rufen Sie diese Nummer an, wird der Anruf von einer Person oder einem Anrufbeantworter beantwortet. Damit können Ihre Kontonummer, Ihre PINs zu verschiedenen Konten, Ihr Kennwörter oder andere persönliche Informationen entlockt und aufgezeichnet werden.

Was kann ich tun, wenn ich Opfer eines Phishing-Angriffs wurde?

Haben Sie bemerkt, dass Sie einem Betrug im Internet zum Opfer gefallen sind? Sobald Sie wissen, dass Sie Opfer einer Phishing-Mail oder -Website geworden sind, sollten Sie umgehend folgende Maßnahmen ergreifen:

- Ändern Sie die Kennwörter oder PINs für alle Online-Konten, die möglicherweise gefährdet sind, und lassen Sie zudem Ihre TAN-Liste sperren – falls Sie eine verwenden.
- Fügen Sie einen Betrugshinweis in Ihre Kreditauskunft ein. Wenn Sie nicht sicher sind, wie das gemacht wird, sprechen Sie mit Ihrer Bank oder Ihrem Finanzberater.

- Wenden Sie sich direkt an die Bank oder den Online-Händler. Informieren Sie unbedingt das betroffene Unternehmen und klicken Sie nicht auf den Link in der betrügerischen E-Mail.
- Wenn eines Ihrer Konten verwendet oder ein Konto in Ihrem Namen eröffnet wurde, schließen Sie diese Konten.
- Überprüfen Sie Ihre Konto- oder Kreditkartenauszüge regelmäßig auf unerklärte Zahlungen oder Anfragen, die nicht von Ihnen stammen.
- Für den Fall, dass die Datendiebe bereits Geld von Ihrem Konto abgebucht haben, hilft nur eine Anzeige bei der Polizei.
- Zusätzlich sollten Sie nicht versuchen, evtl. vorhandene Schadsoftware zu deinstallieren oder Dateien zu reparieren. Diese könnte als Beweismittel für die Polizei benötigt werden.

Quelle: https://www.telekom.de/hilfe/festnetz-internet-tv/sicherheit/phishing?vo=Y0154&wt_mc=em_sesesexx_in2s-es-fnbkp-20220429-d-005&wt_cc3=f1&wt_cc4=m0&samChecked=true