Phishing

Mittels Phishing versuchen Angreifer an Zugangsdaten ahnungsloser Internetbenutzer z.B. zum E-Banking oder zu Online-Shops zu gelangen. Die Täter täuschen dabei eine falsche Identität vor und nutzen so die Gutgläubigkeit ihrer Opfer aus.

Schützen Sie sich vor Phishing, indem Sie...

- nie einen Link verwenden, der per E-Mail, SMS oder Messenger-Dienst zugeschickt oder per QR-Code eingescannt wurde, um sich bei einem Finanzinstitut anzumelden.
- nie Formulare ausfüllen, die per E-Mail zugestellt wurden und zur Eingabe von Anmeldeinformationen auffordern.
- Anhänge von E-Mails und Kurznachrichtendiensten mit grosser Vorsicht behandeln.
- in Telefongesprächen nie vertrauliche Informationen, wie z.B. Passwörter, preisgeben.
- die Adresse zur Anmeldeseite Ihres Online-Dienstleisters oder Finanzinstituts immer manuell in die Adresszeile Ihres Browsers eingeben.
- beim Aufruf der Anmeldeseite die TLS/SSL-Verbindung (https://, Schlosssymbol) überprüfen und sich durch die Kontrolle der Internetadresse in der Adresszeile Ihres Browsers vergewissern, dass Sie sich am richtigen Ziel befinden.
- sich bei Unsicherheit oder Unklarheit an das Finanzinstitut wenden.

(https://www.ebas.ch/phishing-test/)

So läuft ein Phishing-Angriff typischerweise ab

1. Kontaktaufnahme

Kriminelle verschicken gefälschte E-Mails und geben sich als Mitarbeitende von Online-Dienstleistern oder Finanzinstituten aus. Die Empfänger der E-Mails werden beispielsweise darauf hingewiesen, dass die Kontoinformationen oder Zugangsdaten (z.B. Benutzername und Passwort) nicht mehr sicher oder aktuell seien und diese unter dem im E-Mail aufgeführten Link aktualisiert werden sollten.

2. Abfangen persönlicher Daten

Der Link führt allerdings nicht auf die Originalseite des angegebenen Dienstleisters, sondern auf eine gefälschte, jedoch täuschend echt aussehende Webseite. Dort eingegebene, persönliche Informationen, wie beispielsweise Passwörter, gelangen dadurch direkt zur Täterschaft.

3. Bereicherung
Die Kriminellen tätigen dann mit den gestohlenen Informationen im Namen der Opfer beispielsweise Banküberweisungen, kaufen online auf deren Kosten ein oder platzieren gefälschte Angebote bei Online-Auktionsanbietern.

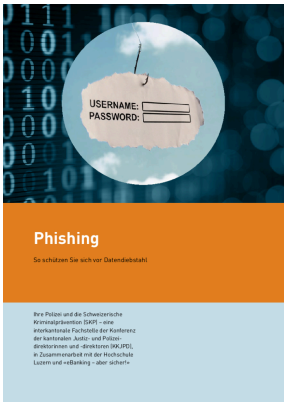
Damit Sie Phishing-Mails erhalten, müssen die Betrüger Ihre E-Mail-Adresse kennen. Um diese Gefahr zu verringern und auch generell den Spam in Ihrem Posteingang zu reduzieren, hilft die Befolgung einiger einfacher Regeln, die Sie in unserem Artikel zum Thema Spam (https://www.ebas.ch/schutz-vor-spam/) finden.

(https://www.antiphishing.ch/de/)

Unter Phishing wird der Diebstahl schützenswerter Informationen wie z.B. Anmeldeinformationen von Internetbenutzern verstanden.

Der Begriff ist ein englisches Kunstwort, welches sich aus «password» und «fishing» zusammensetzt.

Merkblatt:



(https://www.ebas.ch/wp-content/uploads/2019/10/phisingSKP_de.pdf)

Weiterführende Informationen für Interessierte

Klassisches Phishing

Beim klassischen Phishing versuchen die Angreifer ihre Opfer mithilfe von gefälschten E-Mails auf gefälschte Webseiten zu locken und dazu zu bringen, dort ihre Anmeldeinformationen (z.B. Vertragsnummer, Passwort) einzugeben.

Alternativ oder zusätzlich werden oft Mail-Anhänge beigefügt, welche einen Trojaner enthalten, der sich bei öffnen des Anhangs im Hintergrund installiert und fortan die Zugangsdaten des Internetbenutzers ausspioniert oder ihn auf gefälschte Websites führt.

Wichtig zu wissen: Finanzinstitute verschicken nie solche E-Mails!

Prävention: Keine Links oder Anhänge in E-Mails anklicken, sondern die Adresse des Finanzinstituts stets manuell im Browser eingeben. Überprüfung der TLS/SSL-Verbindung und des Zertifikats (https://www.ebas.ch/zertifikatspruefung/) .

Spear Phishing und Dynamite Phishing

Im Gegensatz zum klassischen Phishing, wo grosse Mengen von E-Mails wahllos an ein breites Publikum verschickt werden, werden die Empfänger beim Spear-Phishing gezielt ausgewählt und erhalten E-Mails, die auf sie persönlich zugeschnitten sind.

Der Absender tarnt sich dabei als vertrauenswürdige Person, häufig als Bekannter, Mitarbeiter oder Geschäftspartner des Empfängers. Der massgeschneiderte Inhalt der E-Mails wirkt glaubwürdig und authentisch und wird daher oft auch von Spam-Filtern nicht erkannt.

Werden die personalisierten Mails automatisiert erstellt und massenhaft verschickt, spricht man auch von «Dynamite Phishing».

Prävention: Seien Sie misstrauisch bei unerwarteten E-Mails oder solchen mit ungewöhnlichem Inhalt, auch wenn Sie den Absender zu kennen glauben. Setzen Sie sich mit ihm im Zweifelsfall über einen zweiten Kanal, beispielsweise telefonisch, in Verbindung.

Smishing (SMS-Phishing)

Auch SMS-Nachrichten werden immer öfter für Phishing-Angriffe eingesetzt. Das perfide an «Smishing» ist, dass die meisten Kriterien zur Erkennung von Phishing E-Mails bei SMS-Nachrichten nicht anwendbar sind: Eine persönliche Anrede fehlt meist. Sprache und Gestaltung der Kurznachrichten sind zu einfach und zu knapp, um Rückschlüsse auf eine mögliche Fälschung zu erlauben. Und der wahre Absender sowie der Link lassen sich mit den meisten Mobilgeräten nur schwer überprüfen. Zudem sind sich viele Anwender gewohnt, SMS-Nachrichten zur Verifikation der E-Banking-Anmeldung oder Finanztransaktionen zu erhalten.

Prävention: Klicken Sie niemals auf Links in SMS-Nachrichten, sondern geben Sie die Ihnen bekannte Adresse

der Website des Finanzinstituts von Hand im Browser ein und überprüfen Sie die sichere Verbindung (Schlosssymbol, Zieladresse). Kontaktieren Sie bei unerwarteten SMS-Nachrichten die Bank über die Ihnen bekannten Kontaktinformationen (z.B. offizielle Telefonnummer), und lassen Sie sich den Versand der SMS-Nachricht bestätigen.

Vishing (Phone-Phishing)

Vishing ist die sprachbasierende respektive telefonische Variante des Phishing. Ähnlich wie beim klassischen Phishing werden Benutzer durch gut ausgedachte Geschichten dazu verleitet, vertrauliche Informationen wie z.B. die Anmeldeinformationen fürs E-Banking preiszugeben.

Prävention: Geben Sie vertrauliche Daten wie Passwörter nie einer anderen Person bekannt. Beenden Sie Telefonanrufe, in denen Sie danach gefragt werden, umgehend. Kontaktieren Sie Ihr Finanzinstitut nur über die offiziellen Telefonnummern.

QR-Phishing

Beim QR-Phishing überkleben Angreifer QR-Codes (Quick Response-Codes) an häufig frequentierten Orten durch eigene und führen somit Benutzer auf eine falsche URL. So können ohne Weiteres, insbesondere auf mobilen Geräten, Downloads gestartet, Skripte ausgeführt oder eine gefälschte Login-Seite eines Finanzinstituts angezeigt werden.

Prävention: Verwenden Sie niemals einen QR-Code, um sich bei einem Finanzinstitut anzumelden. Prüfen Sie vor dem Scannen, ob der QR-Codes nicht durch einen gefälschten überdeckt wurde. Überprüfen Sie, ob der Link auf die gewünschte Adresse zeigt.

Phishing mit Webseiten im Anhang

Beim Phishing mit Webseiten ist kein Link oder Dokument in den E-Mails enthalten – stattdessen befindet sich eine gefälschte Webseite als HTM- oder HTML-Datei im Anhang. Das Opfer wird so ausgetrickst, da kein Link mehr anzuklicken ist. Und das Öffnen der Datei im Anhang scheint auf den ersten Blick auch nicht besonders gefährlich zu sein, da es sich nicht um ein Dokument (Word, Excel etc.) handelt, welches z.B. Makros ausführen könnte.

Doch Achtung: HTM- und HTML-Dateien können das Opfer direkt zum Server des Angreifers umleiten! Die eingegebenen Anmeldeinformationen gelangen so in die falschen Hände. Zudem können solche Dateien auch Skripte beinhalten, welche ev. weiteren Schaden verursachen.

In modernen E-Mail-Programmen werden solche Umleitungen und Skripte aus Sicherheitsgründen blockiert. Wenn Sie jedoch einen HTM- oder HTML-Anhang öffnen, unterliegt dieser nicht mehr den Sicherheitseinstellungen des E-Mail-Programms. Das perfide ist zudem, dass sensibilisierte Benutzer ausgetrickst werden, da in der Adresszeile des Browsers «nur» ein lokaler Dateipfad steht und keine dubiose URL wie beim klassischen Phishing.

Prävention: Seien Sie bei HTM- und HTML-Anhängen grundsätzlich skeptisch. Klicken Sie keine Anhänge in E-Mails an, sondern geben Sie die Adresse des Finanzinstituts immer manuell im Browser ein.