ALLES ÜBER PHISHING!

Phishing ist eine der größten Bedrohungen des Internets. Mit gefälschten E-Mails, Web-Seiten, WhatsApp-Nachrichten oder Anrufen sollt ihr betrogen und bestohlen werden.

Welche Phishing-Methoden gibt es?

Der Begriff Phishing leitet sich von „**P**assword **H**arvesting F**ishing**“ ab. Damit ist in erster Linie das „Angeln nach Passwörtern“ gemeint. **Mit einem geeigneten Köder wollen Kriminelle versuchen, euch dazu zu bringen, eure Anmeldedaten fürs Online-Banking und andere Portale herauszurücken.**

- **E-Mail-Phishing**: Dabei werden **bekannte Web-Seiten oft täuschend echt nachgemacht** und die Opfer werden über **gefälschte E-Mails oder Kurznachrichten** dazu gebracht, etwa auf Fake-Bank-Seiten ihre Login-Daten einzugeben.
- **Vishing**: Beim „**Voice-Phishing**“ erhaltet ihr zum Beispiel einen **Anruf mit einer angeblichen Gewinnankündigung**, der sich unterm Strich aber nur als Datendiebstahl oder Versuch herausstellt, euch ein unerwünschtes Abo anzudrehen
- **Smishing**: Noch hinterhältiger ist diese Phishing-Methode, weil **SMS** verwendet werden: Dabei bekommt ihr seltsame Paketankündigungen mit einem Link, der letztlich zu einem **App-Download** führt. Angeblich sollt ihr diese App installieren, um das Paket verfolgen zu können. Tatsächlich handelt es sich aber um einen **Trojaner, der den Verbrechern eure Bank- und andere Zugangsdaten schickt**. Diese Methode beschränkt sich auf Android-Smartphones, weil iPhone-User keine Apps aus fremden Quellen installieren können.
- **Spear Phishing**: Dabei wird gezielt **eine Person innerhalb eines Unternehmens** angegriffen. Mit speziellen, auf diese Person zugeschnittenen E-Mails versuchen die Angreifer, sie zur Herausgabe sensibler Daten oder zur Installation eines Trojaners im Firmennetzwerk zu bringen.

Woran erkennt man Phishing-Versuche?

All diese Methoden haben mehrere gemeinsame Eigenschaften:

- Phishing-E-Mails haben meist eine **unpersönliche Anrede**.
- Ein relativ großer Teil der angesprochenen Personen hat **nicht einmal ein Konto bei dem angeblichen Absender-Portal**.
- Die **E-Mail-Adresse des Absenders** hat meist überhaupt nichts mit dem Unternehmen zu tun, von dem die E-Mail kommen soll.
- Wenn der Text nicht sowieso auf Englisch ist, enthält er oft **zahlreiche Rechtschreibfehler**.
- **Links in der E-Mail gehen**, wenn man sie sich genauer anguckt, **nicht zur offiziellen Web-Seite des angeblichen Absenders**.
- Die **nachgemachten Internetseiten** befinden sich **nicht an der üblichen Adresse des vorgeblichen Absenders**, sondern nutzen entweder gehackte Domains oder Adressen wie https://vr-updates30285.com.
- Bei „**Voice-Phishing-Anrufen**“ sprechen die Anrufer **sehr häufig Deutsch mit einem starken Akzent** und können auf Nachfragen zum Thema keine richtigen Antworten geben. Zweifelt man die gemachten Aussagen an, werden sie zudem häufig beleidigend.
- Außerdem stellt sich ein **Großteil der angezeigten Rufnummern bei einem Rückruf als ungültig** heraus. Durch sogenanntes „Call-ID-Spoofing“ werden Telefonnummern vorgespiegelt, die auf den ersten Blick vertrauenswürdig aussehen. Die Drahtzieher sitzen dabei oft im Ausland.

Wie funktioniert ein Phishing-Angriff?

Am Beispiel eines E-Mail-Phishings wollen wir euch erklären, wie so ein Angriff funktionieren kann.

Ihr erhaltet etwa eine **E-Mail der Volksbank**, die euch (mit fehlerhaftem Text) auffordert, wegen angeblicher neuer Regelungen eure **Bankdaten zu verifizieren**.

1. Es wird gleich **Druck aufgebaut**, indem man beispielsweise droht, dass das Konto nicht mehr genutzt werden kann, bis das geschehen ist.
2. Ein verlinkter Button führt euch zu einer **täuschend echt nachgemachten Volksbank-Seite**, auf der aber kein Link funktioniert und **die Internetadresse auch verdächtig ist**.
3. Hier sollt ihr euch **mit euren Anmeldedaten einloggen**, um angeblich eine Kontoprüfung zu absolvieren.
4. In dem genannten, besonders perfiden Beispiel **gehen die Täter sogar so weit, dass sie im Hintergrund prüfen, ob die Anmeldedaten stimmen**.
5. Danach werden möglicherweise **andere Identifikationsdaten abgefragt** oder man fordert euch auf, **Transaktions-PINs** einzugeben.

Und in diesem Moment sind die Täter so weit, möglicherweise **Zugriff auf euer Konto** zu haben und dort entweder Daten ändern oder **Überweisungen ausführen** zu können. Sie kennen eure Konto- und Kartennummern und können womöglich mit den Anmeldedaten in Shops einkaufen. In anderen Beispielen geht es etwa um die Zugangsdaten zu eurem Mobilfunk-Konto, um euch neue Verträge anzudrehen.

So könnt ihr euch schützen und reagieren

Achtet auf folgende Alarmsignale:

1. Seid ihr **überhaupt Kunde des Absenders**?
2. Wenn **Links** enthalten sind: **Führen sie zur normalen Homepage des Unternehmens**? Falls nicht, ruft die Web-Seite des Unternehmens von Hand auf, seht dort nach, ob von der angekündigten Aktion dort auch die Rede ist und loggt euch normal in euer Konto ein, um dort nach Hinweisen zu suchen. Im Zweifelsfall fragt beim Support nach.
3. Erscheint die **Absender-E-Mail-Adresse plausibel**? Oft genug verwenden die Täter eine beliebige Adresse aus einem Pool gestohlener Adressen.
4. Sind alle **Sätze in dem Anschreiben sinnvoll und fehlerfrei**? Häufig stimmen Kleinigkeiten nicht, die euch aber verdächtig erscheinen sollten.

Falls ihr Opfer eines Phishings geworden seid...

Wenn ihr auf die E-Mail, eine SMS oder einen Anruf hereingefallen seid, müsst ihr schnell handeln.

- Zuerst informiert die Bank beziehungsweise das Unternehmen, dessen Zugangsdaten ihr herausgegeben habt und lasst das Konto sperren.
- Anschließend macht eine Anzeige bei der Polizei – das ist schon aus versicherungstechnischen Gründen notwendig.
- Zuguterletzt ändert eure Zugangsdaten und tut das auch in allen anderen Zugängen, bei denen ihr dummerweise dieselbe Kombination aus Benutzernamen oder E-Mail-Adresse und Passwort benutzt habt.