

Phishing

Als Phishing bezeichnet man das Erschleichen von [personenbezogenen Daten](#), wie Name und Anschrift sowie Kontodaten und Kreditkartendaten, um damit Straftaten begehen zu können. Über Phishing werden auch Zugangsdaten für Bankkonten, Kundenzugänge bei Zahlungsdienstleistern wie Paypal oder Accounts der sozialen Netzwerke oder Online Shops erbeutet.

- Dynamit-Phishing: [Angriff](#) mit [Spam](#) an zehntausende [Empfänger](#) gleichzeitig, auch durch Schadsoftware, kein gezielter [Angriff](#) gegen Einzelnen, sondern über Masse, es reicht, wenn Erfolgsquote für Angreifer bei 0,2 % liegt
- [Spear-Phishing](#): Menschliche Schwäche ausnutzen, Zugangsdaten entlocken: Der [Angriff](#) ist gegen ein Opfer persönlich gerichtet. Es werden individuell auf das Opfer abgestimmte, präparierte Dateien oder Dokumente [verwendet](#).

Zu einer Phishing Attacke gehören mehrere Komponenten, eine [Spam](#) Mail, eine präparierte Webseite und Menschen, die auf den Schwindel reinfallen.

Der Versand der [Spam](#) Mails erfolgt mittels entsprechender Tools zum Versand von Massenmails mit Funktionen zur Manipulation von Absender und technischen [Daten](#). Grundlage sind in der Regel erbeutete [Daten](#), mindestens von E-Mail Adressen. Oft werden auch noch Anreden sowie Name und bei gut vorbereiteten Attacken Anschriften [verwendet](#). Oft sind die Spamwellen von mehreren 10.000 Mails jedoch auch unpersönlich ohne spezifische Anrede in der [Spam](#).

Dabei wird mit einer präparierten Mail vorgestäuscht, dass bei einem Kundenkonto einer Bank, eines Zahlungsdienstleisters oder sonstigen Anbieters ein kritisches Sicherheitsproblem besteht.



In dieser Mail wird vorgestäuscht, dass es ein Problem mit einem Paypalkonto gibt. Absender der elektronischen Post ist angeblich das [Unternehmen](#), mit dessen Konto es angeblich kritische Sicherheitslücken geben soll. Die Beispielsmail hat keine spezifische Anrede. Es wird bei Phishing Mails immer der Eindruck beim Opfer erzeugt, dass bestimmte Handlungen notwendig sind, um eine Gefahr abzuwenden. Diese Hanlungen bestehen im Eingeben von [Daten](#) in einer präparierten Webseite oder das Öffnen von Dateien, die dann Schadsoftware enthalten.

Die Mail im Beispiel wurde von einem Spamfilter als unerwünschte Massenmail bereits aussortiert und in den [Spam](#) Ordner eines Postfaches eingeordnet. Die Mail enthält einen Link auf eine präparierte Webseite. Interessant ist der Inhalt und Verhalten der präparierten Webseite.



Klickt man den Link an, landet man nicht, wie behauptet auf einer Unterseite des Zahlungsanbieters Paypal, sondern auf der präparierten Webseite des Hackers. Die Seite sieht aus, wie die Webseite von Paypal. Erkennbar ist die Phishing Attacke nur an der "Url" in der Eingabezeile des Browsers. Der Link leitet auf eine Seite "privatkunden.de-web3432.pw" weiter und nicht auf die Originaldomain paypal.com. Phishing Attacken sind daran immer erkennbar. Ein forensisch arbeitendes Antivirenprogramm sollte vor solchen Links deutlich warnen.

Die präparierte Webseite besteht aus mehreren Unterseiten. Als erstes wird eine Log In Seite aufgerufen. Hier - für Paypal ungewöhnlich - werden Nutzernamen und Passwörter untereinander abgefragt. Bei Paypal wird mittels Script erst der Nutzernamen abgefragt und kontrolliert. Erst in einem zweiten Schritt wird auf der selben Seite das Passwort vom Nutzer verlangt. Im Beispiel fehlte dieser Prozess. Auffallend war hier, dass man jeden Buchstaben eingeben konnte und immer auf die nächste Unterseite weitergeleitet wurde. Es gab keinerlei Fehlermeldungen.



Auf der nächsten Unterseite werden der Name und die Anschrift abgefragt. Die [Daten](#) werden dann unter anderem für Bestellungen in Online Shops oder zur Erstellung neuer Kundenkonten missbraucht. Nachdem das Opfer auch diese Felder ausgefüllt hat und auf weiter klickt, werden die Bank- und Kreditkartendaten abgefragt. Diese [Daten](#) werden genutzt, um die Konten abzuräumen oder anderweitig zu missbrauchen. Die eingegebenen [Daten](#) werden mittels Script oft in Datenbanken oder in csv Dateien abgespeichert. Die meisten Hacker verschlüsseln weder den Zugriff auf die Dateien, noch verhindern sie den Zugriff darauf mittels Passwort.

Phishing erfüllt mehrere Straftatbestände, unter anderem wegen des

- Versands der [Spam-Mails](#) § [269 StGB](#),
- Erstellen der Phishing-Website § [269 StGB](#), §§ 143, 143a [MarkenG](#) bzw. §§ 106 ff. [UrhG](#), wenn markenrechtlich bzw. urheberrechtlich geschützte Kennzeichen oder Bezeichnungen [verwendet](#).
- anschließende [Datenverwendung](#) § [202a StGB](#) strafbar, Zugang zu den Konto- und Depotinformationen
- Verwendung der [Daten](#) für Onlineüberweisung nach § [263a StGB](#) und §§ 269, [270 StGB](#)

Datenschutz praktische
Lektion



[Zur Buchung \(EUR 7,00 / 1 Monat\)](#)

[7 Min Datenschutz](#) **juristi.e-Seminar**

Aus- und Weiterbildung