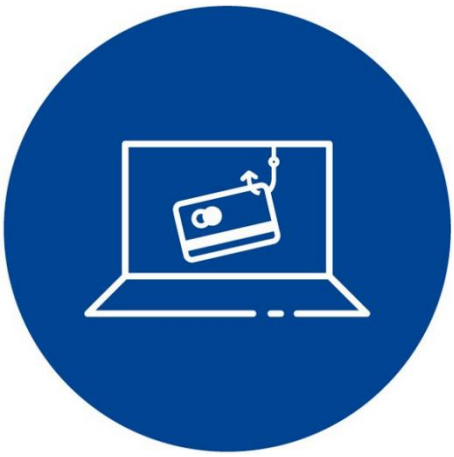
Rat und Hilfe für Verbraucher in Europa

ECC-Net

Europäisches Verbraucherzentrum Italien

PHISHING



Herausgegeben vom

Europäischen Verbraucherzentrum Italien - Büro Bozen

Brennerstraße 3 I-39100 Bozen

Tel. +39-0471-980939 Fax +39-0471-980239

www.euroconsumatori.org

info@euroconsumatori.org

Facebook
Centro Europeo Consumatori Italia

Twitter
ECC Italy

Instagram
ecc.italy

YouTube
Centro Europeo Consumatori Italia

Finanziell unterstützt durch die Europäische Union

I n h a l t e

Das Europäische Verbraucherzentrum Italien wird mit gefördert durch die Generaldirektion für die Harmonisierung des Marktes und den Verbraucherschutz des Ministeriums für die wirtschaftliche Entwicklung, durch die Generaldirektion Justiz,Verbraucher und Gleichstellung der Europäischen Kommission,durch das Land Südtirol und die Autonome Region Trentino-Südtirol, und ist Mitglied im Netzwerk der Europäischen Verbraucherzentren (ECC-Net). Trägerorganisationen sind die Verbraucherzentrale Südtirol und die Verbraucherorganisation Adiconsum.

Diese Publikation wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union finanziert(2014-2020). Der Inhalt dieser Publikation gibt ausschließlich die Ansicht des Europäischen Verbraucherzentrums Italien wieder und liegt in dessen alleiniger Verantwortung. Er spiegelt nicht den Standpunkt der Europäischen Kommission und/oder der Exekutivagentur für Verbraucher, Gesundheit,Landwirtschaft und Lebensmittel (CHAFEA) oder einer anderen Einrichtung der Europäischen Union wider. Die Europäische Kommission und die Agentur übernehmen keinerlei Verantwortung für eine mögliche Verwendung von Informationen, die dieser Publikation zu entnehmen sind.Die Informationen dieser Publikation sind mit größter Sorgfalt recherchiert und aufgearbeitet worden, dennoch kann keine Garantie für eventuelle Fehler übernommen werden. Die in der vorliegenden Publikation beinhalteten Informationen können nur als Richtlinien und als Teilinformationen betrachtet werden.

Stand März 2021

Phishing: Was ist das?

Phishing ist ein **Betrug**, der im Internet durch Täuschung der Benutzer durchgeführt wird. Der Betrüger sendet eine **E-Mail**, die vorgibt, von einem bekannten und vertrauenswürdigen Unternehmen gesendet worden zu sein, und versucht, die Empfänger zur Angabe von **persönlichen Informationen, Passwörtern**, **Zugangsdaten** zu Online-Banking-Seiten und/oder Finanzdaten zu verleiten.

Woher kommt der Begriff “phishing”?

Der Begriff Phishing ist eine Variante von *fishing* (dies bedeutet im Englischen “fischen”) und weist darauf hin, dass mit immer ausgefeilteren Techniken nach den sensiblen Daten eines Nutzers "gefischt" wird. Das Wort kann auch mit der Sprache Leet (dort werden Buchstaben beispielsweise durch Ziffern ersetzt) zusammenhängen sein, wo der Buchstabe “f” häufig durch “ph” ersetzt wird.

Wie funktioniert es?

Phishing erfolgt häufig in Form von **irreführenden E-Mails**, die scheinbar von Finanzinstituten wie Banken oder Kreditkartenunternehmen stammen, oder von Webseiten, die eine Registrierung erfordern, wie z. B. E-Commerce-Seiten oder Web-Mails.

Indem die Nachricht meldet, dass es Registrierungs- oder andere Probleme gibt, fordert sie dazu auf, Zugangsdaten für den Dienst anzugeben. In der Regel enthält die Nachricht einen **Link** zur Webseite des Kreditinstituts oder des Dienstes, bei dem der Benutzer registriert ist, um ihn in falscher Sicherheit zu wiegen. Tatsächlich scheint die Webseite, zu der eine Verbindung hergestellt wird, identisch mit der ursprünglichen Webseite, es handelt sich aber um eine **Fälschung**. Falls der Nutzer seine vertraulichen Daten eingibt, sind sie für Kriminelle zugänglich.

Phishing erfolgt manchmal auch über **SMS**, **Social Media-Nachrichten** oder über Nachrichten, die mittels **Instant Messaging-Plattformen** empfangen werden.

Eine weitere Gefahr des Phishings

Eine Gefahr geht vom Einsatz von **Computerviren** aus mit dem gleichen Ziel, Zugangsdaten für Online-Finanzdienste oder andere Dienste, die eine Registrierung erfordern, zu stehlen.

Es gibt mehrere Möglichkeiten der Infizierung. Am häufigsten geschieht dies über einen **E-Mail-Anhang**. Neben Dateien mit der Endung .exe werden Viren auch über gefälschte Rechnungen, Bußgeldbescheide, Paketzustellungsnachrichten verbreitet, die auch im .doc- oder .pdf-Format sein können.

Im Fall von "*financial malware*" (also Finanz-Schadsoftware) oder "*trojan banking*" (Banking-Trojaner, also auf das Banking spezialisierte Viren) wird der Virus aktiviert, um **Finanzdaten** zu **stehlen**, ohne dass diese bereitgestellt werden müssen.

Andere Arten von Viren, die "*Keylogger*" (dabei handelt es sich um eine Hard- oder Software, mit der die Eingaben auf der Tastatur eines Computer protokolliert werden), werden aktiviert, wenn *User*-ID (Benutzer-Identifikation) und Passwort auf der Tastatur eingegeben werden. **In diesem Fall gelangen die Kriminellen in den Besitz der Zugangsdaten zu unseren E-Mail- oder E-Commerce-Konten**.

Das Phishing ist so angelegt, dass es leicht ist, in die Falle zu tappen

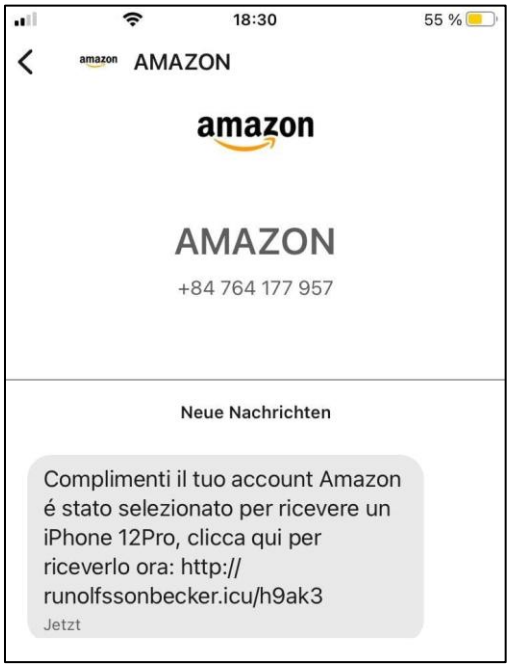
Täglich bekommen wir jede Menge E-Mails. Viele davon sind Werbung und zahlreiche landen direkt im **Spam-Filter**.

Kriminelle Hacker nutzen hauptsächlich E-Mails für ihre Phishing-Angriffe. Mit der nötigen Vorsicht können Sie **verdächtige E-Mails erkennen**. Es handelt sich dabei fast immer um E-Mails mit einem **gefälschten Logo**, die den Empfänger auffordern, eine bestimmte Webseite zu besuchen, um vertrauliche Daten wie Kreditkartennummer oder Zugangsdaten anzugeben. Diese Webseiten haben eine nahezu perfekte Ähnlichkeit mit den richtigen Webseiten und sie verleiten den Benutzer dazu, auf die Links in der E-Mail zu klicken. Ein Beispiel dafür wäre eine Nachricht von einer Webseite, die sich als ein Datenunternehmen ausgibt, wie z. B. Aruba, und Sie auffordert, Ihr Abonnement zu verlängern oder Ihre Kontodaten zu erneuern, indem Sie auf einen Link klicken.

Bei vielen dieser Nachrichten ist die Grafik so vertraut, dass es nicht schwer ist, in die Falle zu tappen. Sie könnten z. B. von einem Hacker eine E-Mail zur Erneuerung Ihres E-Mail-Kontos erhalten, der dieselbe Grafik und Schriftart wie die geklonte Webseite verwendet.

Möglicherweise erhalten Sie von einem Freund eine E-Mail, in der dieser Ihnen mitteilt, dass er sich im Ausland befindet und dass ihm seine Dokumente, das Geld und das Handy gestohlen wurden; er bittet Sie, ihm mit *Money Gram* oder *Western Union* Geld zu senden. Sie tappen in die Falle und geben Ihre Kontakte, den Zugang zu Ihren digitalen Profilen, Geld und, im schlimmsten Fall, die Zugangsdaten zu Ihren Bankkonten an betrügerische Seiten weiter.

Mit der Entwicklung von **sozialen Netzwerken** und **Instant Messaging-Plattformen** sind es oft auch andere Instrumente, mit denen kriminelle Hacker versuchen, uns in die Phishing-Falle zu locken. Zum Beispiel könnten Sie über Telegram eine Nachricht von Amazon erhalten, mit dem gleichen Logo wie das multinationale Unternehmen, und der Aufforderung, auf einen Link zu klicken, um ein neues Handy zu erhalten, nachdem Sie als Gewinner eines Wettbewerbs ausgewählt wurden ... Aber dann hat die Telefonnummer, von der die Nachricht ankommt, die Vorwahl eines Landes, das Sie nicht erwarten würden, zum Beispiel Vietnam, wie im hier dargestellten Fall:



Wie entlarvt man Phishing? - Praktische Tipps

Die gute Nachricht ist, dass es **Software** gibt, die diese Art von **Betrug entlarven kann**. Wir empfehlen Ihnen zu prüfen, ob Sie eine Erweiterung für den von Ihnen verwendeten Browser herunterladen können, die ähnlich aussehende Adressen entlarvt. Sie wird in einigen Fällen zugelassen, indem sie dem Browser aus dem Webstore hinzugefügt wird. Ihre Funktion ist einfach, aber potenziell sehr nützlich: Wenn man versucht, mit einer "Lookalike"-Adresse (also einer ähnlich aussehenden Adresse) auf eine Webseite zuzugreifen, fragt sie uns, ob wir das wirklich tun wollen. An diesem Punkt würde selbst ein abgelenkter Benutzer die **URL** richtig lesen und die Täuschung entlarven.

Viele Webseiten, die Online-Dienste anbieten, bei denen Sie sich anmelden müssen (Anbieter von E-Mail- und PEC-Adressen, E-Commerce-Seiten, die Steuerbehörde...), informieren über die Gefahr von Phishing und geben wertvolle Tipps, wie Sie Phishing erkennen und vermeiden können.

Im Allgemeinen sind folgende Vorsichtsmaßnahmen zu beachten:

- **Überprüfen Sie, ob Sie sich auf der echten Seite befinden**. Wenn Sie auf einen Link klicken, kontrollieren Sie sorgfältig in der Browserleiste, ob Sie nicht auf einer verdächtigen Adresse gelandet sind. Auch wenn sie den Original-Webseiten grafisch sehr ähnlich sind, weist der Name der Seite oft kleine Unterschiede in der Adresse im Vergleich zur echten Seite auf.

- **Verwenden Sie die Adressleiste des Browsers**. Im Zweifelsfall sollten Sie niemals gewöhnlichen E-Mails vertrauen, die Links enthalten. Es ist besser, die eigenen Konten direkt zu überprüfen, indem Sie auf die offiziellen Webseiten gehen und die Adresse in die Leiste Ihres Browsers eingeben.

- **Überprüfen Sie die E-Mail-Adresse des Absenders.** Wenn Ihnen eine E-Mail verdächtig vorkommt, überprüfen Sie, ob die Adresse wirklich zu der Person gehört, von der sie angeblich stammt. Wenn der Absender z. B. Apple ist, aber die E-Mail-Adresse YYX@352-apple.com lautet, sollten Sie vorsichtig sein.

- **Achten Sie auf Fehler.** In den plumpsten Fällen von Phishing enthalten die E-Mails Rechtschreibfehler oder kleine Umstellungen im Namen des vermeintlichen Absenders. In jedem Fall ist die Adresse, von der diese E-Mails kommen, eine andere als die offizielle. Seiten wie paypall.com anstelle von paypal.com oder gcogle.com anstelle von google.com enthalten geringfügige Unterschiede im Vergleich zur echten Adresse. Sie werden verwendet, um Benutzer auszutricksen, denen das Detail des verschiedenen Buchstabens entgeht, und die ihre Online-Zugangsdaten eingeben, die in der Folge gestohlen werden.

- **Schenken Sie Dringlichkeiten keinen Glauben.** Das ist einer der Faktoren, welchen sich Phishing am meisten zu nutze macht: eine ausstehende Zahlung, die sofort beglichen werden muss, ein Gewinn, der schnell abgeholt werden muss, oder das Risiko, ein Konto zu verlieren, wenn man nicht sofort zahlt. Wenn eine E-Mail Sie in Eile versetzt, ist das Risiko, dass es sich um einen Betrug handelt, hoch.

- **Achten Sie auf Anhänge.** Bei Anhängen mit den Endungen .pfd, .doc., .exe oder anderen eher ungewöhnlichen, oder zumindest nicht erwarteten, Endungen sollten Sie sehr vorsichtig sein. In diesem Fall könnten sich hinter diesen Dateien neben einfachem Phishing auch Viren verstecken.

- **Niemand hat etwas zu verschenken.** E-Mails, in denen Geldgewinne oder Preise jeglicher Art bekanntgegeben werden, sind fast immer gefälscht. Ein Smartphone für 1 Euro, die Erbschaft eines entfernten Verwandten oder ein Lottogewinn sollten immer die Alarmglocken läuten lassen.