Alias-Adresse

Kettenbriefe

Spam

Hoax

Searchbots

Wegwerf-Identität

E-Mail-Harvesting

Phishing

Phishing, betrügerische Webshops oder gestohlene Daten sind ärgerliche Nebenerscheinungen des Internets. Laut dem Internet-Sicherheitsbericht 2013 von Cert.at steigen die Gefahren von Onlinekriminalität, während das Bewusstsein für die Risiken vieler hinterherhinkt. Userinnen und User können sich jedoch mit einfachen Mitteln vor Spam, Phishing und kommerziellem Onlinebetrug schützen.

Onlinebetrug

Spam

Fast jede E-Mail-Adresse, die über eine gewisse Zeit in Gebrauch ist, wird früher oder später von unerwünschten Massenaussendungen heimgesucht, in denen von Potenzmitteln bis zu brachliegenden, aber prall gefüllten Konten bei Londoner Banken beinahe alles beworben wird. Spam verursacht in der weltweiten Onlinekommunikation großen Schaden, der auf die immense Datenmenge und den Aufwand der Bekämpfung zurückzuführen ist.

Die Zusendung von Werbemails an private Adressen ist ohne vorherige Zustimmung der Adressatin oder des Adressaten nicht erlaubt. Das gilt umso mehr für Zusendungen an mehr als 50 Personen, deren Einwilligung nicht vorliegt. Jedoch sieht das Gesetz eine Ausnahme vor: Unternehmen dürfen E-Mail-Werbung verschicken, wenn Userinnen und User zuvor bei ihnen etwas erworben haben und nicht die Zusendung von Werbemails aktiv abgelehnt haben. Das Unternehmen muss aber jederzeit die Gelegenheit bieten, weitere Zusendungen abzulehnen. Standardmäßig sind diese „Ausstieg-Links" in den Werbemails enthalten.

Ursprünglich wurde lediglich das ***USENET*** nach E-Mail-Adressen durchkämmt. Später wurden sogenannte ***SEARCHBOTS*** entwickelt, die das Internet nach allem absuchten, was nach einer E-Mail-Adresse aussah. Um sich diesem ***E-MAIL-HARVESTING*** zu entziehen, reicht es daher, die eigene E-Mail-Adresse nirgends öffentlich im Internet zu hinterlassen oder diese derart zu schreiben, dass Programme diese schwerer als Adressen identifizieren können (max[Punkt]mustermann [at]gmx[Punkt]at). Mit dem Aufkommen von ***VIREN*** war es aber bald möglich, einen befallenen Computer nach E-Mail-Adressen zu durchkämmen und diese „nach Hause zu telefonieren" – also an Dritte zu übermitteln.

Werden dennoch unerlaubt und ohne Zustimmung Werbemails verschickt, kann gegen die Absenderin oder den Absender Anzeige beim für das jeweilige Bundesland zuständigen Fernmeldebüro erstattet werden. Das wird jedoch bei Werbemails aus dem Ausland kaum helfen können. In diesem Fall ist auch davon abzuraten, ein E-Mail mit einer Abmelde- oder Ablehnungs-

Spam:
(Urspr. ein Markenname für Dosenfleisch, das während des Zweiten Weltkriegs als einziges Nahrungsmittel im Überfluss erhältlich war.) Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere Massenaussendungen mit Werbung.

Usenet:
Eigenständiges, weltweites elektronisches Netzwerk, welches lange vor dem World Wide Web entstand. Jenes Netz, in dem die klassischen Diskussionsforen des Internets (Newsgroups) zu Hause sind.

Searchbots:
Auch Spider oder Webcrawler genannt, sind Computerprogramme, die das Internet durchsuchen und Webseiten analysieren; sie werden vor allem zum Sammeln von E-Mail-Adressen, RSS-Newsfeeds und anderen Informationen eingesetzt.

erklärung zu schicken – denn wird auf Spam reagiert, erfahren die Spammerinnen und Spammer, dass sie eine gültige E-Mail-Adresse gefunden haben, und schicken im schlimmsten Fall noch mehr davon.
Der beste Schutz vor Spam ist Vorsorge. Es empfiehlt sich, zwei verschiedene E-Mail-Adressen zu führen: eine für berufliche und eine für private Zwecke. So kann auch das berufliche Ich vom privaten Ich getrennt werden.
Die berufliche E-Mail-Adresse sollte ausschließlich für Geschäftszwecke genutzt werden und sonst nicht weitergegeben werden. Denn eine Adresse, die nirgends öffentlich aufscheint, ist für Spammerinnen und Spammer deutlich schwerer zu bekommen.
Die private E-Mail-Adresse kann für Registrierungen bei sozialen Netzwerken, Newsletter und Gewinnspiele verwendet werden. Sie kann auch bei Bedarf leichter gewechselt werden. Es empfiehlt sich, für die Privatadresse einen großen Webmail-Anbieter zu wählen, da diese in der Regel über gute Spamfilter verfügen.

Tipp
Zwei E-Mail-Adressen zu haben bedeutet nicht zwingend, dafür zwei verschiedene Anbieter zu nutzen. Größere Mail-Provider bieten an, mehrere E-Mail-Adressen gleichzeitig zu verwenden, die dennoch in einem Postfach zusammengeführt werden. So können Userinnen und User sehr leicht ihren beruflichen und privaten E-Mail-Verkehr über ein Postfach verwalten.

Eine weitere Möglichkeit, sich vor Spam zu schützen, ist, für Anmeldungen bei Onlinediensten eine ***ALIAS-ADRESSE*** oder eine ***WEGWERF-ADRESSE*** zu verwenden. Viele Onlinedienste prüfen die Identität nicht, verlangen aber dennoch eine Datenangabe. Diese E-Mail-Adressen werden automatisch generiert und funktionieren nur für einen kurzen Zeitraum – lang genug, um die Registrierung durchzuführen. So werden keine „Datenspuren" hinterlassen.

Neben dem Angebot von Generatoren solcher Wegwerf-E-Mail-Adressen gibt es auch Generatoren für erfundene Identitäten. Per Zufallsgenerator wird eine fiktive Identität mit Namen, Geburtsdatum und Adresse erstellt. Dieser Service kann beispielsweise zum Schutz der Privatsphäre genutzt werden, aber auch, um Mängel schlecht konstruierter Webseiten und ausländischer Onlinedienste auszugleichen. Beispielsweise verweigert ein amerikanischer Onlinedienst die Anmeldung mit österreichischer Adresse, da die hiesigen Postleitzahlen vierstellig sind, das Eingabefenster aber für amerikanische, neunstellige Postleitzahlen konzipiert ist.

E-Mail-Harvesting:
(„To harvest", Engl. für ernten.) Automatisiertes Sammeln von E-Mail-Adressen aus Foren, Dokumenten und von Webseiten.

Viren:
Schädliche Computerprogramme, die sich selbstständig einschleusen und verbreiten können.

Fernmeldebüros:
www.bmvit.gv.at/telekommunikation/organisation/nachgeordnet/fmb

E-Mail-Dienste:
www.mail.google.com
www.mail.yahoo.de

Alias-Adresse:
(Engl. „alias" für Deckname oder Pseudonym.) E-Mail-Adresse, die keinen Hinweis auf die eigene Identität gibt.

Wegwerf-Adresse:
Wegwerf-E-Mail-Adressen sind provisorische E-Mail-Adressen, die nur für einen bestimmten Zeitraum gültig sind und anschließend verfallen.

Wegwerf-Identität:
Mit „Fake Identity"-Generatoren werden per Zufallsgenerator willkürlich Name, Geburtsdatum und Adresse aus Datenbanken ausgewählt.

Welche Schutzmaßnahmen zur Abwehr von Spam-Mails können getroffen werden?

- → ***Vorsorge:*** *Die eigene E-Mail-Adresse sollte nicht im Internet veröffentlicht werden; mit abonnierten Newslettern, Teilnahme an Gewinnspielen und Registrierung bei Webseiten steigt die Wahrscheinlichkeit für Spam. Ebenso empfiehlt es sich, verschiedene E-Mail-Adressen zu verwenden, beispielsweise eine für berufliche und eine für private Zwecke.*
- → ***Spamfilter beim Provider:*** *Die meisten Provider bieten einen solchen mittlerweile kostenlos an. Diese Spamfilter kennzeichnen den Spam (z. B. im Betreff) oder sortieren ihn automatisch in einen eigenen Ordner (z. B. Spam- oder Junk-Ordner).*
- → ***Spamfilter auf dem eigenen Computer:*** *Eine weitere Möglichkeit zur Abwehr ist ein Spamfilter auf dem eigenen Computer, die meisten E-Mail-Programme bieten sehr gute selbst lernende Spamfilter an; mit diesem Filter kann auch Spam aussortiert werden, der beim Provider durchgerutscht ist – der Spamfilter des Providers ist grobmaschiger, da damit viele Personen gleichzeitig bedient werden müssen.*
- → ***Robinsonliste:*** *Weiters besteht die Option, sich in die sogenannte Robinsonliste der RTR eintragen zu lassen. Das ist eine Liste mit den Kontaktdaten von Personen, die keine unangeforderte Werbung erhalten möchten. Zum Eintragen genügt ein formloses E-Mail an eintragen@ecg.rtr.at mit dem Betreff „Eintragen RTR-ECG-Liste"; diese Liste schützt jedoch nur bedingt vor Spam, da sich viele Spammerinnen und Spammer nicht an die rechtlichen Vorschriften halten.*
- → ***Achtung:*** *Userinnen und User sollten dennoch regelmäßig in ihren Spam-Ordner hineinsehen, da es vorkommen kann, dass das eine oder andere „echte" E-Mail darin landet.*

Phishing

Phishing ist eine Betrugsvariante, bei der Kriminelle versuchen, an Nutzerinformationen – beispielsweise Passwörter oder Zugangsdaten für Onlinebanking – heranzukommen. Die am weitesten verbreitete Form ist hierbei Datendiebstahl über E-Mail. In der Regel werden E-Mails verschickt, die den Anschein offizieller Nachrichten echter Unternehmen haben. In dem E-Mail werden die Userinnen und User aus einem vermeintlich wichtigen Grund dazu aufgefordert, einen Link anzuklicken, ihre Kontodaten neu einzugeben oder den Anhang zu öffnen.

Die meisten Phishing-E-Mails sind mittlerweile hochprofessionell und können oftmals auf den ersten Blick nicht als Betrug identifiziert werden. Eine andere Variante des Phishing ist, dass beim Öffnen des E-Mail-Anhangs

Phishing:
(Kunstwort aus „fishing", Engl. für fischen, und „password", Engl. für Passwort.) Betrugsmasche, um an Zugangsdaten zu kommen und somit Zugriff zu Accounts und Konten zu erhalten.

ein Virus oder ein Trojaner heruntergeladen wird, der im Hintergrund alle Tätigkeiten beobachtet und sofort „nach Hause telefoniert", sobald wertvolle Zugangsdaten oder -informationen eingetippt werden. Ebenso wurden aber auch Fälle gemeldet, bei denen sich telefonisch Unbekannte bei Nutzerinnen und Nutzern meldeten und sich z.B. als Mitarbeiter eines Computerunternehmens ausgeben. Sie behaupteten, einen Virus auf dem Computer entdeckt zu haben un d forderten die Nutzerin oder den Nutzer auf ihre Zugangsdaten durchzusagen. Seit dem Strafrechtsänderungsgesetz 2015 ist Phishing strafrechtlich erfasst und kann mit einer Freiheitsstrafe von bis zu einem Jahr verhängt werden, bei gewerbsmäßigem Phishing sogar bis zu drei Jahre.

Phishing
§ 241h Abs. 1 StGB

Wie können Phishing-E-Mails erkannt werden?

- → ***Faustregel:*** *Kein seriöses Unternehmen wie eine Bank oder ein Onlineshop fragt Daten der Kundinnen und Kunden per E-Mail ab oder tritt überhaupt über sehr allgemeine E-Mail-Aussendungen mit ihnen in Kontakt. Im Zweifelsfall sollte direkt die Webseite der Bank oder des Onlineshops besucht werden, oftmals sind dort bereits Hinweise auf aktuelle Betrugsmaschen zu finden.*
- → ***Absende-Adresse:*** *Wenden sich seriöse Unternehmen an ihre Kundinnen und Kunden – beispielsweise die Bankberaterin oder der Bankberater –, wird eine E-Mail-Nachricht auch entsprechend von der E-Mail-Adresse einer Person kommen (z. B. susanne.musterfrau@beispielbank.at) und nicht von einer allgemeinen E-Mail-Adresse; ein weiterer Hinweis kann sein, dass die E-Mail-Adresse besonders lang ist, aus Buchstaben- und Zahlenkombinationen besteht oder keiner österreichischen .at-Domain angehört, beispielsweise aus Polen, der Ukraine oder Russland kommt (.pl, .ua oder .ru).*
- → ***Original und Fälschung:*** *Professionelle Phishing-Mails imitieren bekannte Firmennamen oder deren Mail-Adressen. Beispielsweise kommt ein E-Mail statt von der echten Mail-Adresse der Bank Austria - office@unicredit-group.at – von einer auf den ersten Blick identisch aussehenden, bei der lediglich ein Buchstabe anders ist: office@unikreditgroup.at. Es empfiehlt sich, genau hinzusehen, um nicht getäuscht zu werden.*
- → ***Falsche Links:*** *Um diese zu erkennen, sollten Userinnen und User vor dem Anklicken den Mauszeiger darüberbewegen, unten links auf dem Bildschirm wird daraufhin der gesamte Linkpfad angezeigt; ist hier zu erkennen, dass es sich beispielsweise um einen Link auf eine ausländische Seite handelt, obwohl das E-Mail scheinbar aus dem Inland kommt, sollten Userinnen und User vorsichtig sein.*
- → ***Webadressen:*** *Um sicherzugehen, dass es sich auch tatsächlich um die richtige Webseite handelt, sollte die Webadresse eigenhändig in den Browser eingegeben werden.*

Stopp dem Internetbetrug.

Kostenlose Tipps für Ihre Sicherheit!

Machen Sie den Schritt zu mehr Sicherheit.

Das Sicherheitsportal der Bank Austria hält für Sie umfassende Informationen bereit – zum Beispiel aktuelle Tipps, wie Sie Betrugsversuche beim OnlineBanking erkennen.

http://sicherheit.bankaustria.at

Das Leben ist voller Höhen und Tiefen. Wir sind für Sie da.

Willkommen bei der
Bank Austria
Member of UniCredit

- → ***Sicherere Verbindung:*** *Bei der Eingabe von Daten im Internet sollte immer auf eine sichere Verbindung geachtet werden, also eine SSL-verschlüsselte Internetverbindung; hierbei wird der Webadresse https:// vorangestellt, im Browser erscheint neben der Webadresse das Schlosssymbol.*
- → ***Unpersönliche Anschreiben:*** *Seriöse Unternehmen schreiben ihre Kundinnen und Kunden persönlich an, unpersönliche Anreden wie „Guten Tag" oder „Sehr geehrte/r Kunde und Kundin" können ein Hinweis auf Phishing sein.*
- → ***Sprachliche Qualität:*** *Früher waren Phishing-Nachrichten auf den ersten Blick am schlechten Deutsch zu erkennen. Obwohl sich das mittlerweile geändert hat, können sich noch der eine oder andere Fehler oder eigenartige Formulierungen finden lassen.*
- → ***Textbaustein suchen:*** *Erscheint ein E-Mail verdächtig, kann es hilfreich sein, einen kleinen Textausschnitt daraus mittels Suchmaschine im Internet zu suchen. Meistens sind Phishing-Mails bereits weit verbreitet, und es gibt Warnungen und Artikel darüber zu finden (z. B. Hoax-Info-Service der TU Berlin (hoax-info.tubit.tu-berlin.de).*
- → ***Watchlist Internet:*** *Diese unabhängige österreichische Plattform informiert regelmäßig und aktuell über die neuesten Internetfallen. Hier können Nutzerinnen und Nutzer auch Fälle von Spam, Phishing etc. melden.*

Watchlist Internet
www.watchlist-internet.at

Hoax/Kettenbriefe/419 Scam

Hoax:
(„Hoax", Engl. für Scherz oder Schwindel.) Falschmeldung, die Userinnen und User täuschen soll, damit diese die Meldung weiterverbreiten.

419 Scam:
Sammelbezeichnung für verschiedene Betrugsvarianten per E-Mail, leitet sich vom entsprechenden Paragrafen des nigerianischen Strafgesetzes ab, da viele dieser Betrugsbanden ihren Sitz in Nigeria haben.

Ein Hoax ist eine Falschmeldung, die über E-Mail, Instant Messenger, soziale Netzwerke oder andere Wege verbreitet wird. Oftmals hat diese Meldung den Anschein einer authentischen Warnung vor Internetgefahren – beispielsweise vor Viren oder auch, sehr beliebt, einer Änderung der Nutzungsbedingungen auf Facebook – und wird daher von vielen freiwillig weitergeleitet. Die vergleichsweise harmloseren Kettenbriefe sollen nur Panik und Unsicherheit verbreiten, besonders Kinder sind hierfür anfällig. Bösartige Hoaxes sollen Nutzerinnen und Nutzer in Fallen locken, indem sie zusätzlich noch Abhilfe versprechende Links mitschicken, die jedoch nur Viren oder Malware bescheren oder zu betrügerischen Webseiten führen. Über aktuelle Hoaxes informiert beispielsweise die österreichische Plattform Watchlist Internet (www.watchlist-internet.at) oder der Hoax-Info-Service der TU Berlin (hoax-info.tubit.tu-berlin.de).

Kommerzieller Onlinebetrug

Den größten Schaden richten kommerzieller Onlinebetrug und betrugsähnliche Internetfallen an. Eine sehr verbreitete Form von Onlinebetrug sind

Webshops, die billige Markenware (z. B. Kleidung, Elektronik) anbieten. Hier sollten Nutzerinnen und Nutzer besonders misstrauisch sein, denn auch im Internet wird nichts verschenkt. Diese Betrugsform tritt üblicherweise in zwei Spielarten auf: Entweder handelt es sich statt um Originalware um billige Fälschungen (Produktpiraterie), oder die bestellte Ware kommt nach der Zahlung niemals an. Oftmals werden diese Webshops unter Angabe falscher Daten gegründet, viele davon sind in China angesiedelt. In den vergangenen Jahren hat sich auch der Onlinebetrug mit Immobilien gehäuft. Hierbei werden schöne Wohnungen in guter Lage und zu niedrigen Preisen beworben, doch die vermeintlichen Glücksgriffe existieren nicht. Unter einem Vorwand fordert die angebliche Verkäuferin oder der angebliche Verkäufer, manchmal aber auch die beauftragte Immobilienagentur, Geld für eine Besichtigung oder eine Kaufanzahlung, das angeblich bei Nichtgefallen rückerstattet wird. Oftmals ist das Geld, das die Interessierten überweisen, gar nicht das eigentliche Ziel, sondern die Bankdaten der unwissenden Userinnen und User.

Wie können Betrugsseiten erkannt werden?

- → ***Faustregel:*** *Internationale und vertrauenswürdige Unternehmen führen oft eigene europäische, wenn nicht sogar österreichische Webshops (z. B. H&M, Amazon). Bei Anbietern außerhalb der EU oder ohne europäische Verkaufsplattform sollten Nutzerinnen und Nutzer vorsichtig sein, da es hier unter Umständen schwierig sein kann, ihr Recht durchzusetzen. Jedoch ist nicht jede Webseite mit einer .at- oder .de-Domain vertrauenswürdig! Bei Domainnamen, die Schlagwörter wie „Outlet" oder „Sale" enthalten, ist Vorsicht geboten.*
- → ***Impressum:*** *Das Impressum kann Aufschluss darüber geben, wer die Eigentümerin/der Eigentümer dieser Domain ist. Webshops, die keine entsprechenden Informationen offenlegen, sollten mit Vorsicht behandelt werden.*
- → ***Rücktrittsrecht:*** *Vertrauenswürdige Unternehmen haben AGB und erläutern darin das Rücktrittsrecht.*
- → ***Vorauskassa meiden:*** *Zahlungen im Voraus sollten tunlichst vermieden werden. Mittlerweile gibt es verschiedene sichere(re) Online-Bezahlmethoden, die von den meisten Webshops unterstützt werden. Ebenso sollte bei unbekannten Webshops erst nach dem Erhalt der Ware das Geld überwiesen werden.*
- → ***Aufmerksam lesen:*** *Viele Anbieter arbeiten mit der Unachtsamkeit der Käuferinnen und Käufer. Durch die richtigen Schlagwörter und Bilder in der Produktbeschreibung soll der Eindruck vermittelt werden, dass es sich beispielsweise um ein iPad handelt, jedoch wird bei genauerem Lesen lediglich eine iPad-Hülle verkauft.*
- → ***E-Commerce-Gütezeichen:*** *Dieses Gütezeichen kennzeichnet seriöse Onlineshops, die zuvor auf Sicherheit und Kundenservice geprüft wurden.*