Datenklau im Internet

In Betrug-Mails werden Opfer aufgefordert, Passwörter und Zugangsinfos preiszugeben

Das Thema

Einbrüche, Enkeltrick, Phishing, Scamming und Internetbetrug, die Tricks der Kriminellen werden immer raffinierter, und die Opferzahlen steigen. In Kooperation mit der Polizei klären wir auf und geben Tipps zur Prävention.

Von Bea Ricken

Daten am Haken: Betrüger versuchen per Mail an Kreditkartennummern und Passwörter zu kommen. Foto: Andrea Warncke/Archiv

WOLFHAGER LAND. Schlechtes Deutsch und schräge Sätze sind längst kein Erkennungsmerkmal mehr für sogenannte Phishing-Mails, die bei internetaktiven Menschen mittlerweile fast täglich im Eingangsordner landen. Sie kommen angeblich von Banken, Paypal, der Telekom, sozialen Netzwerken, Internetverkäufern wie Amazon oder sogar dem Bundesamt für Sicherheit und haben sogar die persönliche Anrede.

Als bei einer Polizistin aus Kassel die betrügerische Mail der Sparkasse aufploppte, stutzte sie – obwohl berufsbedingt sensibilisiert – dennoch einen kurzen Moment: „Diese Mail war nicht nur optisch sauber gestaltet, sondern auch sprachlich fast völlig in Ordnung. Mir fiel aber dann sofort auf, dass dort Sparkasse stand und nicht die Kasseler Sparkasse, bei der ich Kunde bin“, erzählt die Polizeibeamtin, die nicht genannt werden möchte. Sie leitete die Betrugsmails an ihre Kollegin Aniane Emde von der Präventionsabteilung weiter.

Aniane Emde

„Die Methoden der Betrüger werden immer raffinierter“, warnt Emde. „Kamen früher Mails im Umlauf, die einfach gestrickt und schlecht formuliert die Absicht des Absenders auf Anhieb verrieten, so ködern die Täter ihre Opfer heute mit professionell gestalteten Mails, die selbst von Profis nur schwer als Fälschung zu identifizieren sind.“ Ziel sei es immer, den Empfänger zu veranlassen, persönliche Daten wie Zugangsdaten, Passwörter und Transaktionsnummern preiszugeben.

„Niemals wird die Kasseler Sparkasse ihre Kunden per E-Mail dazu auffordern, solche Daten preiszugeben beziehungsweise abzugleichen“, betont denn auch der Pressesprecher der Kasseler Sparkasse, Michael Krath, zu den jüngsten Betrugsversuchen. Warnhinweise würden Kunden auch auf der Homepage der Bank finden.

„Im Moment sind auch Phishing-Mails im Umlauf, bei denen das Opfer sogar aufgefordert wird, den Personalausweis einzuscannen“, so Emde. Die Täter können mit den hochgeladenen Personaldokumenten zusätzlichen Missbrauch betreiben. Solche Daten werden zum Beispiel für betrügerische Verkäufe bei Immobilien oder Fahrzeuge eingesetzt.

Informationen welche Betrugsmails gerade im Umlauf sind, gibt es beim Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen.

http://zu.hna.de/Phishingradar

HINTERGRUND

Abfischen von Passwörtern

Bei dem Wort „Phishing“ handelt es sich um ein Kunstwort, zusammengesetzt aus den englischen Worten „password“ und „fishing“. Wörtlich übersetzt bedeutet es so viel wie das Abfischen von Passwörtern. Doch nicht nur Passwörter bringen die Betrüger trickreich in Erfahrung. Auch an weiteren persönlichen Daten wie Name, Geburtstag, Anschrift oder aber Bank-Zugangsinformationen sind die Datenklauer interessiert.

Mit diesen persönlichen Daten können Betrüger mit der vorgegaukelten Identität im Namen des Geschädigten online nahezu alle Geschäfte abwickeln (Geld überweisen, Dispokredit ausschöpfen, Online-Einkäufe tätigen). (ewa)

Quelle: Polizei


leider konnten wir von Ihnen seit dem 21.12.2017 keinen Zahlungseingang feststellen.

Ihr Anschluss wird daher gemäß unseren Allgemeinen Geschäftsbedingungen für weitere Nutzung ab dem 22.02.2018 gesperrt. Damit Sie Ihren Anschluss weiter vollständig nutzen können, begleichen Sie bitte die beigelegte Rechnung umgehend.

Sollte die Zahlung bereits erfolgt sein, betrachten Sie diese E-Mail bitte als gegenstandslos.

Mit freundlichen Grüßen

Telekom Deutschland GmbH

So sehen sie aus: Die Betrüger drohen in Phishing-Mails mit der Sperrung von Telefonanschlüssen und Konten. Bewusst wird psychischer und zeitlicher Druck aufgebaut. Screenshots: Polizei/privat

„Erst checken, dann klicken“

Polizei warnt davor, persönliche Daten oder Passwörter im Internet zu übermitteln

Wie bei Betrugsversuchen an der Haustür oder auf der Straße sollte man auch im Interent auf sein Bauchgefühl hören, rät Reinhard Giesa, Chef der Präventionsabteilung beim Polizeipräsidium Nordhessen. Gegenüber elektronischer Post sei immer ein gesundes Misstrauen angebracht. Besonders wenn in vermeintlich echt aussehenden Mails zeitlicher oder psychischer Druck aufgebaut werde. „Lassen Sie sich nicht locken, folgen Sie nicht blind irgendwelchen Anweisungen in Emails - erst checken, dann klicken“, appelliert Giesa.

Reinhard Giesa

Weitere Tipps:

- Vergewissern Sie sich, mit wem Sie es zu tun haben. Überprüfen Sie die Adressleiste in Ihrem Browser. Bei geringsten Abweichungen sollten Sie stutzig werden.
- Klicken Sie niemals auf den angegeben Link in der übersandten E-Mail. Versuchen Sie stattdessen, die in der E-Mail angegebenen Seiten tatsächlich auch über die Startseite Ihrer Bank zu erreichen.
- Kreditinstitute fordern grundsätzlich keine vertraulichen Daten per E-Mail oder per Telefon oder per Post von Ihnen an. Wenn Sie sich unsicher sind, halten Sie Rücksprache mit Ihrer Bank.
- Übermitteln Sie keine persönlichen oder vertraulichen Daten wie Passwörter oder Transaktionsnummern per Mail.
- Folgen Sie Aufforderungen in E-Mails, Programme herunterzuladen, nur dann, wenn Sie die entsprechende Datei auch auf der Internet-Seite des Unternehmens finden (Starten Sie keinen Download über den direkten Link). Öffnen Sie keine angehängten Dateien.
- Geben Sie persönliche Daten nur bei gewohntem Ablauf innerhalb des Online-Banking Ihres Kreditinstituts an. Sollte Ihnen etwas merkwürdig vorkommen, beenden Sie die Verbindung und kontaktieren Sie Ihre Bank.
- Beenden Sie die Online-Sitzung bei Ihrer Bank, indem Sie sich abmelden.
- Kontrollieren Sie regelmäßig Ihren Kontostand sowie Ihre Kontobewegungen. So können Sie schnell reagieren, falls ungewollte Aktionen stattgefunden haben.
- PIN und TANs sollten Sie nur dann eingeben, wenn eine gesicherte Verbindung mit Ihrem Browser hergestellt ist, die Sie zuvor selbst über die Startseite ihrer Bank und keinesfalls über eine zuvor erhaltene Email hergestellt haben.

Quelle: Polizei

Weitere Infos im Internet unter

www.polizei-beratung.de
www.polizei.hessen.de/Praevention