„Man darf dem Täter kein Gesicht geben“ >
< Menschen ermutigen, die sich einmischen

Phishing – so können Sie sich schützen

Internetkriminelle wollen an ihre Zugangsdaten für Online-Geschäfte gelangen

E-Mail-Anfragen zu Kreditkartendaten sollten ignoriert und sofort gelöscht werden

„Phishing“ ist ein Kunstwort, das sich aus den englischen Begriffen „Password“ (=Passwort) und „Fishing“ (=Angeln, Fischen) zusammensetzt. Bei diesem Betrugsversuch im Internet werden E-Mails verschickt, die oberflächlich einen seriösen Eindruck erwecken. Tatsächlich geht es nur um das Abgreifen von persönlichen Daten. Opfer dieser Masche sind sowohl Privatpersonen als auch Unternehmen.
Im privaten Bereich gaukeln die E-Mails meist vor, sie kämen von der Hausbank des Nutzers. Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) kennt man diese Betrugsmasche genau: „Als seriöse Bank oder Unternehmen getarnt fordern die Betrüger den Empfänger in der E-Mail auf, seine Daten zu aktualisieren, entweder weil zum Beispiel die Kreditkarte ablaufe, das Passwort erneuert werden müsse oder die Zugangsdaten verloren gegangen seien“, erläutert Nora Basting vom BSI. „Der Inhalt der Phishing-Mails wirkt dabei täuschend echt. Diese E-Mails im HTML-Format zeigen dann einen „offiziellen“ Link an, hinter dem sich jedoch tatsächlich die Verbindung zu einer ganz anderen, nämlich gefälschten Internetseite verbirgt. Um diesen tatsächlichen Link zu entdecken, muss man den Quelltext der HTML-Mail lesen. Das klingt kompliziert, funktioniert aber recht einfach über einen Klick mit der rechten Maus-Taste im Nachrichtenfeld und der Auswahl des Menüpunktes "Quelltext anzeigen"“.
Wer einer gefälschten Seite seine EC-Geheimnummer, Kreditkartennummer oder andere Daten anvertraut, der beschert dem Internet-Angler fette Beute und kann sich selbst jede Menge Ärger einhandeln. Die BSI-Expertin rät daher zu großer Wachsamkeit: „Banken und Unternehmen wissen, dass

E-Mails von Betrügern nur allzu leicht gefälscht werden können. Daher werden sie ihre Kunden niemals per E-Mail dazu auffordern, irgendwo im Internet vertrauliche Daten einzugeben. Der beste Schutz ist also, vorsichtig zu sein und erst gar keine Daten preiszugeben. Reagieren Sie nicht auf E-Mails, die Sie auffordern, auf Webseiten persönliche Daten einzugeben und öffnen Sie zum Schutz vor Schadsoftware niemals Anhänge von E-Mails, die Ihnen verdächtig vorkommen“, sagt Nora Basting. Man kann als Nutzer davon ausgehen, dass praktisch alle E-Mails von vermeintlichen Banken, die sensible Daten abfragen wollen, Betrug sind.
Neben den „klassischen“ Phishing-Mails werden Zugangsdaten immer häufiger über Trojanische Pferde abgegriffen, die sich bei ungenügendem Schutz vor Schadsoftware auf dem Rechner installieren können und im Internet eingegebene Daten und Passwörter mitlesen. Da ein solcher Identitätsdiebstahl per Schadsoftware meist für den Nutzer nicht zu bemerken ist, sind hier vorbeugende Schutzmaßnahmen besonders wichtig.

Wie schützt man sich?

„Aktuelle Software und Vorsicht im Umgang mit persönlichen Daten sind das A und O zum Schutz des Rechners“, rät Nora Basting vom Bundesamt für Sicherheit in der Informationstechnik. Dazu gehören auch sichere Passwörter, die in regelmäßigen Abständen geändert werden. Als relativ sicher gelten individuelle alphanumerische Kombinationen mit mindestens acht Zeichen, also eine Mischung aus Zahlen, Buchstaben und Sonderzeichen. Zur Software-Grundausstattung zählen ein Antivirenschutzprogramm und eine Personal Firewall. Daneben ist ein Anti-Spyware-Programm empfehlenswert. „All dies ist aber nur wirkungsvoll, wenn die Programme immer auf dem neuesten Stand gehalten werden. Das gilt auch für das Betriebssystem des Computers und Anwendungsprogramme wie den Internet-Browser. Hier müssen die angebotenen Sicherheitsupdates regelmäßig – am besten automatisch – installiert werden.“ Weitere Informationen rund um das Thema IT-Sicherheit finden sich auf der Internetseite BSI für Bürger des Bundesamts für Sicherheit in der Informationstechnik.

Nora Basting

Sprecherin des BSI © Bundesamt für Sicherheit in der Informationstechnik

Woran Sie eine Phishing-Mail erkennen:

- Vorsicht, wenn Sie das Unternehmen gar nicht kennen! Hatten Sie noch nie mit dem Unternehmen zu tun, ist die E-Mail wahrscheinlich Spam und schlimmstenfalls sogar eine Phishing-Mail.
- Bei der Kommunikation mit ihren Kunden folgen Dienstleistungsunternehmen bestimmten Regeln. So wird z. B. eine Bank niemals ihre Kunden dazu auffordern, vertrauliche Daten über einen Internet-Link einzugeben oder per E-Mail zu senden.
- Beachten Sie die Betreff-Zeile! Ein seriöses Unternehmen wird niemals in einer E-Mail den Betreff "Konto_Überprüfung_ HEUTE" wählen. Dienstleistungsunternehmen kennen die Namen ihrer Kunden! Die meisten Phishing-E-Mails sind dagegen unpersönlich gehalten und nutzen allenfalls Anreden wie etwa „Lieber Kunde“ oder „Lieber Nutzer“.
- Schauen Sie sich die E-Mail-Adresse an! Viele Betrüger „verpacken“ ihre E-Mail-Adresse in Namen bekannter Unternehmen. Spätestens ein Klick auf diesen Namen enthüllt die tatsächliche E-Mail-Adresse.

In seinem Newsletter informiert das Bundesamt für Sicherheit in der Informationstechnik regelmäßig über IT-Sicherheitslücken, bspw. zum Thema Phishing. Aktuelle Phishing-Warnungen veröffentlicht auch die Verbraucherzentrale NRW auf ihrer Webseite.

- Zunehmend sind Phishing-Mails auch personalisiert und besser ausformuliert. Dadurch sind sie noch schwieriger zu identifizieren. Umso wichtiger ist eine gesunde Skepsis des Nutzers. Kontaktieren Sie im Zweifelsfall ihre Geschäftspartner direkt und fragen Sie nach, ob die Mail auch wirklich von ihm stammt.

Folgende Artikel könnten Sie auch interessieren:

- Gefährlicher als Phishing?
- Kontaktloses Bezahlen
- Romance Scamming – der Liebesbetrug
- Smartphones sind Wertsachen
- Internetkriminalität auf jeden Fall anzeigen!
- Malware und Spyware - „Stars“ der Internetkriminalität
- Zehn Tipps zu Ihrer Sicherheit im Internet

Alle Artikel dieser Kategorie

Weitere Infos für Eltern

Kontaktbeamte für muslimische Institutionen leisten Netzwerkarbeit

„Was man nicht kennt, macht einem Angst“

Kontaktbeamte und -beamtinnen für muslimische Institutionen (KMI)...[mehr erfahren]

Vertrauen ist gut, Kontrolle ist besser

Was tun bei unberechtigten Kontoabbuchungen?

Wer viel im Internet einkauft, kann bei seinen Zahlungen und...[mehr erfahren]

Werden jugendliche Täter von den Gerichten zu mild bestraft?

„Die beste Kriminalpolitik ist eine gute Sozialpolitik“

Sind die von deutschen Gerichten verhängten Strafen für jugendliche...[mehr erfahren]

Eine Initiative für mehr Sicherheit in der Schule

„Schule gegen sexuelle Gewalt“

Anfangs freute sich die 15-jährige Schülerin, als ihr Sportlehrer ihr...[mehr erfahren]

Der Girls’ Day im Polizeipräsidium Köln

Mädchen lernen „Männerberufe“ kennen

In vielen Ausbildungsberufen und Studiengängen in den Bereichen IT,...[mehr erfahren]
