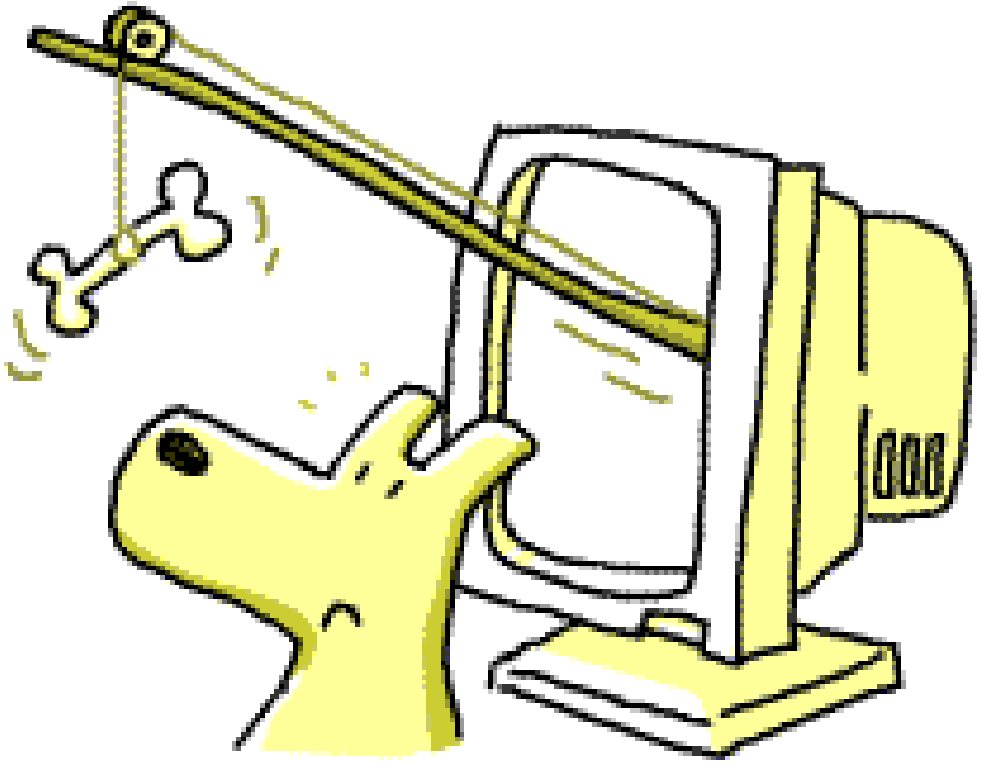
Phishing



Alexander Meister, Maria Buzov,
Christoph Quenkert

Phishing

- Was bedeutet oder ist Phishing?
- Wie funktioniert Phishing?
- Schutzmaßnahmen
- Woran erkennt man Phishing?
- Beispiele

Was bedeutet oder ist Phishing?

- „Password“ und „fishing“ = Phishing
  → Auf Deutsch: „nach Passwörtern angeln“

- Phishing-Betrüger fälschen E-Mails und Internetseiten, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern zu gelangen – die Nutzer geben ihre Daten einfach „freiwillig“ preis.

- Nicht mehr nur auf Internet beschränkt – mittlerweile machen Datendiebe auch schon Jagd auf Nutzer über das Telefon unter Verwendung von Internettelefon (VoIP)

Wie funktioniert Phishing?

- Angreifer verfassen E-Mails, die in Aussehen und Inhalt jenen von z.B. Banken gleichen.
- Sie spekulieren darauf, dass der Empfänger der massenweise verschickten Nachrichten tatsächlich Kunde dieser Firmen ist.
- Das Opfer wird verleitet, einen in der E-Mail enthaltenen Internetlink zu verfolgen, welcher auf eine gefälschte Webseite dieser Firma führt.
- Gibt das Opfer dort vertrauliche Daten ein, „fischen“ die Betrüger diese ab und greifen selbst auf das Konto zu.

Wie funktioniert Phishing?

- Formal gesehen passiert ein Angriff in zwei Etappen:
  - Zum einen über eine E-Mail, welche ein Vertrauensverhältnis ausnutzt. Sie lockt auf eine bösartige Internetseite oder hat Computerschädlinge im Schlepptau. Heute sind diese oft perfekt formuliert.
  - Zum anderen gibt es die Nachahmung von Webseiten, auch „Spoofing“ genannt. Der eigentliche Betrug erfolgt hier, indem der getäuschte Nutzer zur Preisgabe vertraulicher Daten verleitet wird, die dann missbraucht werden.

Schutzmaßnahmen

- Software immer auf dem aktuellen Stand halten:
  - Aktualisierungen („Patches“) so schnell wir möglich vom Hersteller herunterladen und installieren. Bei vielen Herstellern über automatische Update- und Warndienste.
  - Wichtige Neuerungen auch im Newsletter „Sicher Informiert“ des BSI, der alle zwei Wochen veröffentlicht wird [www.buerger-cert.de].
- Sicherheitsstatus von Webseiten überprüfen, auf denen persönliche Informationen eingegeben werden:
  - Auf gesicherten Seiten erscheint in der Statuszeile des Browsers ein Schlosssymbol. Hier kommt das Verschlüsselungsverfahren SSL zum Einsatz. Bei einem klick auf das Symbol erscheint ein „Zertifikat, welches von einer anerkannten Stelle ausgestellt worden sein muss. Die Bundesnetzagentur ist als Behörde dafür zuständig.
  - Darauf achten, dass die in der Adresszeile angegebene URL mit „https“ beginnt, da es ein starke Indiz für eine SSL-Verbindung ist.

Schutzmaßnahmen

- Banken oder seriöse Firmen fordern ihre Kunden niemals per E-Mail oder Telefon zur Eingabe von vertraulichen Informationen auf:
  - Sie wissen, das E-Mails von Betrügern leicht gefälscht werden können, daher fordern sie ihre Kunden niemals per E-Mail auf, angeführte Links anzuklicken und vertrauliche Daten einzugeben.
  - Das gleiche gilt für Telefonate. Firmen wenden sich nie von sich aus und fordern einen zur Eingabe von Passwörtern etc. auf.
- Bank oder Firma kontaktieren, wenn befürchtet wird, einen Phishing-Angriff zum Opfer gefallen zu sein:
  - Für die Sicherheitsfragen zuständigen Mitarbeiter können den Vorfall verfolgen und prüfen, ob schaden entstanden ist.
  - Falls bereits Summen unberechtigt überwiesen worden sind, so ist sich umgehend an die Polizei zu wenden.

Schutzmaßnahmen

- Generelle Sicherheitsregeln für das Internetsurfen und den E-Mail-Verkehr sind zu beachten:
  - Niemals auf in E-Mails enthaltene Links klicken, sondern die gewünschte URL manuell eintippen.
  - Nicht auf vermeintliche Anrufe der Bank reagieren, in denen man zur Eingabe von PIN oder TAN aufgefordert wird.
  - Funktion „Aktive Inhalte ausführen“ generell ausschalten, bzw. über die Sicherheitseinstellung im Browser Funktion aktivieren, das jedes mal explizit gefragt wird, ob aktive Inhalte ausgeführt werden sollen.
  - E-Mails und darin enthaltene Anhänge nur öffnen, wenn diese aus vertrauenswürdigen Quellen stammen.
  - Firewall und Virenschutzsoftware einsetzen und regelmäßig auf aktuellen Stand bringen.
  - Softwareaktualisierungen für Betriebssystem und anderen Programmen laufend installieren oder automatische Update-Dienste verwenden.

Woran erkennt man Phishing?

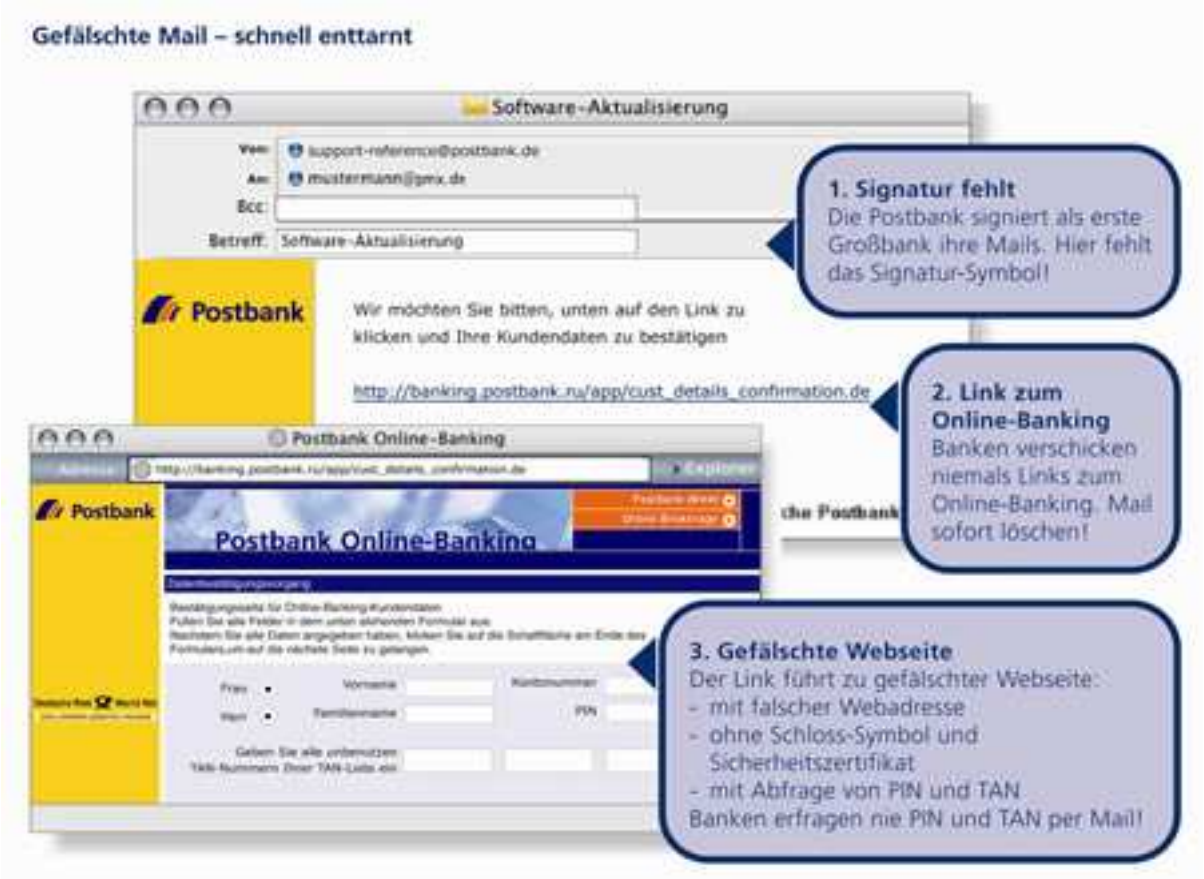
- Phishing E-Mails:
  - Absenderadressen sind zumeist gefälscht. Erkennung ist nur über die Header-Auswertung möglich.
  - Anrede ist unpersönlich gehalten („Lieber Kunde von...“).
  - Dringender Handlungsbedarf wird signalisiert („Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren...“).
  - Drohungen kommen zum Einsatz („Wenn Sie das nicht tun, sperren wir Ihr Konto...“).
  - Vertrauliche Daten werden abgefragt z.B. in einen Formular innerhalb der E-Mail.
  - Mails enthalten Formulare oder Links, die vom Empfänger verfolgt oder geöffnet werden sollen.
  - Die Nachrichten sind manchmal in schlechtem Deutsch verfasst, da sie manchmal von anderen Sprachen per Computer automatisch übersetzt werden.
  - Die E-Mails enthalten kyrillische Buchstaben oder falsch aufgelöste bzw. fehlende Umlaute.

Woran erkennt man Phishing?

- Phishing Webseiten:
  - Oft fehlt in der Adresszeile des Browsers das Kürzel „https“, das eine gesicherte Verbindung signalisiert. Allerdings kann auch das schon manchmal gefälscht sein.
  - Es erscheinen Internetadressen, die den echten ähnlich sind, allerdings Zusätze enthalten wie z.B. www.x-bank.servicestelle.de.
  - Auf der Login-Seite werden TAN-Codes abgefragt.
  - Das Sicherheitszertifikat, erkennbar durch das Schlosssymbol in der Statusleiste, fehlt oder ist gefälscht.

Beispiele Postbank

Beispiele Postbank

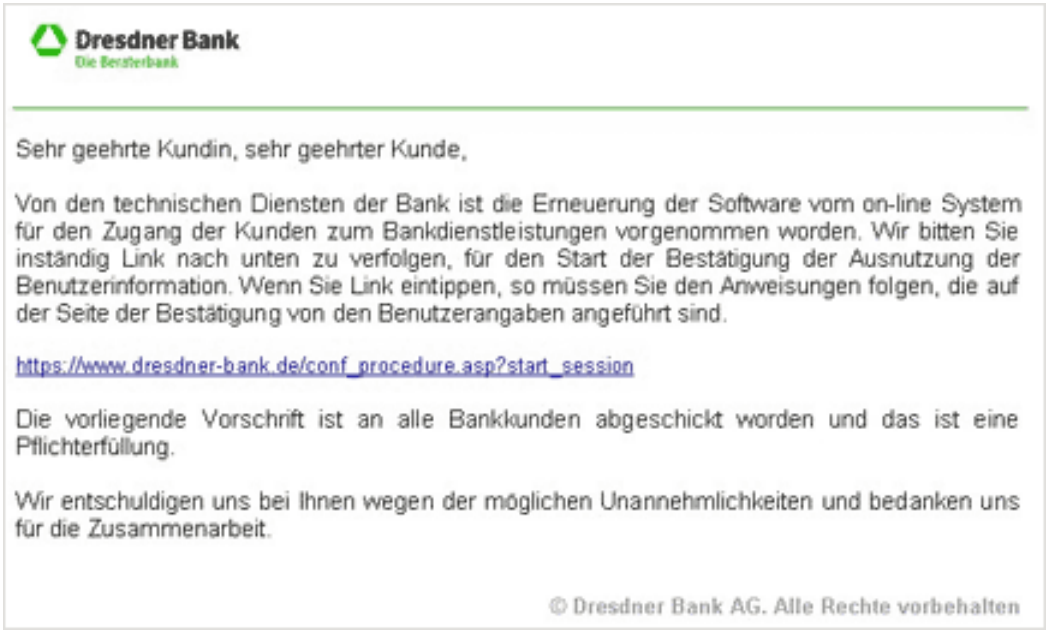


Beispiele Postbank

Beispiele Postbank

Gefälschte Postbank Webseite

Beispiele Dresdner Bank



Dresdner Bank
Die Bestenbank

Sehr geehrte Kundin, sehr geehrter Kunde,

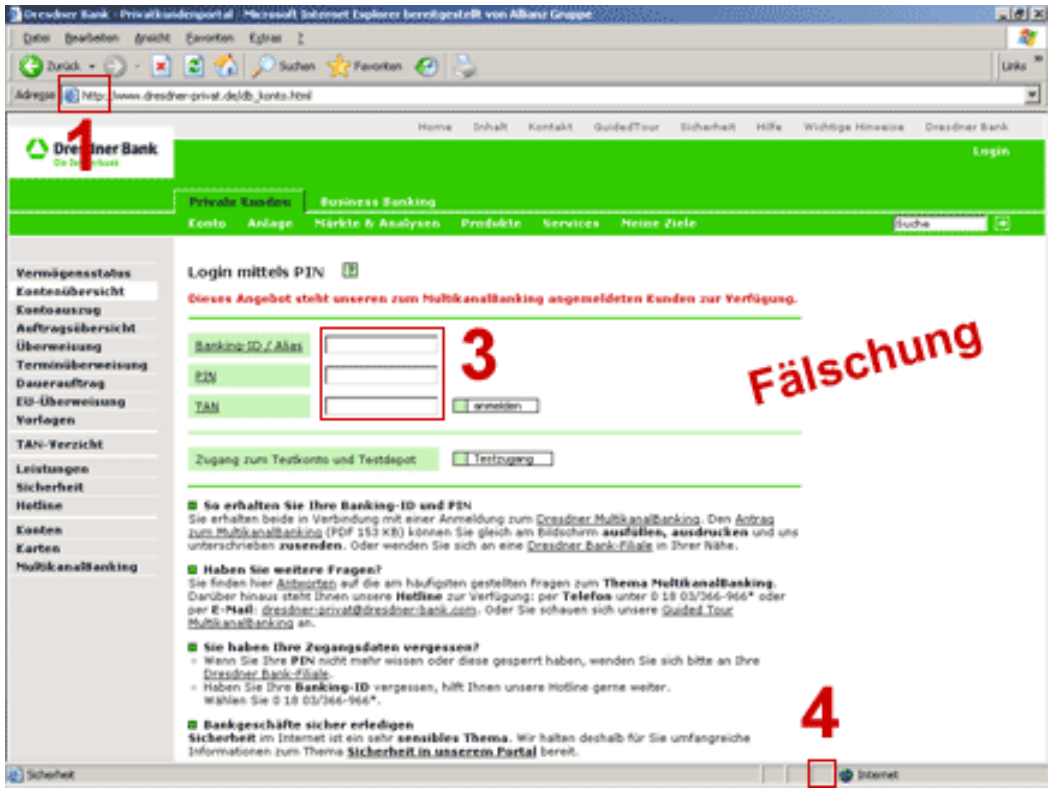
Von den technischen Diensten der Bank ist die Erneuerung der Software vom on-line System für den Zugang der Kunden zum Bankdienstleistungen vorgenommen worden. Wir bitten Sie inständig Link nach unten zu verfolgen, für den Start der Bestätigung der Ausnutzung der Benutzerinformation. Wenn Sie Link eintippen, so müssen Sie den Anweisungen folgen, die auf der Seite der Bestätigung von den Benutzerangaben angeführt sind.

https://www.dresdner-bank.de/conf_procedure.asp?start_session

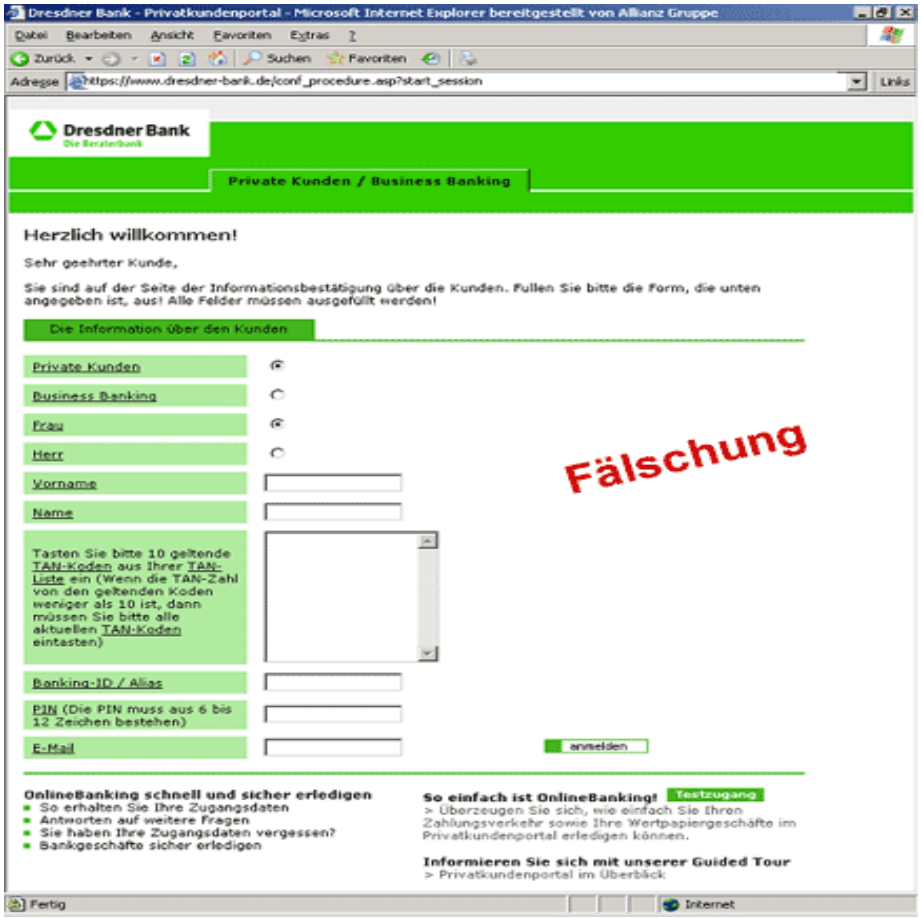
Die vorliegende Vorschrift ist an alle Bankkunden abgeschickt worden und das ist eine Pflichterfüllung.

Wir entschuldigen uns bei Ihnen wegen der möglichen Unannehmlichkeiten und bedanken uns für die Zusammenarbeit.

Beispiele Dresdner Bank



Beispiele Dresdner Bank



Quellen / weitere Infos

- Quellenangaben:
  - Internetseite der „Bundesamt für Sicherheit in der Informationstechnik“: http://www.bsi-fuer-buerger.de

- Weitere Infos:
  - In Deutschland gibt es eine interdisziplinarische Vereinigung aus Wissenschaftlern der Ruhr-Universität Bochum, die sich das Phishing-Problem angenommen haben. Die „Arbeitsgruppe Identitätsmissbrauch im Internet“ stellt online aktuelle Informationen zur IT-Sicherheit bereit sowie auch konkrete Hilfestellungen und Tools. https://www.a-i3.org