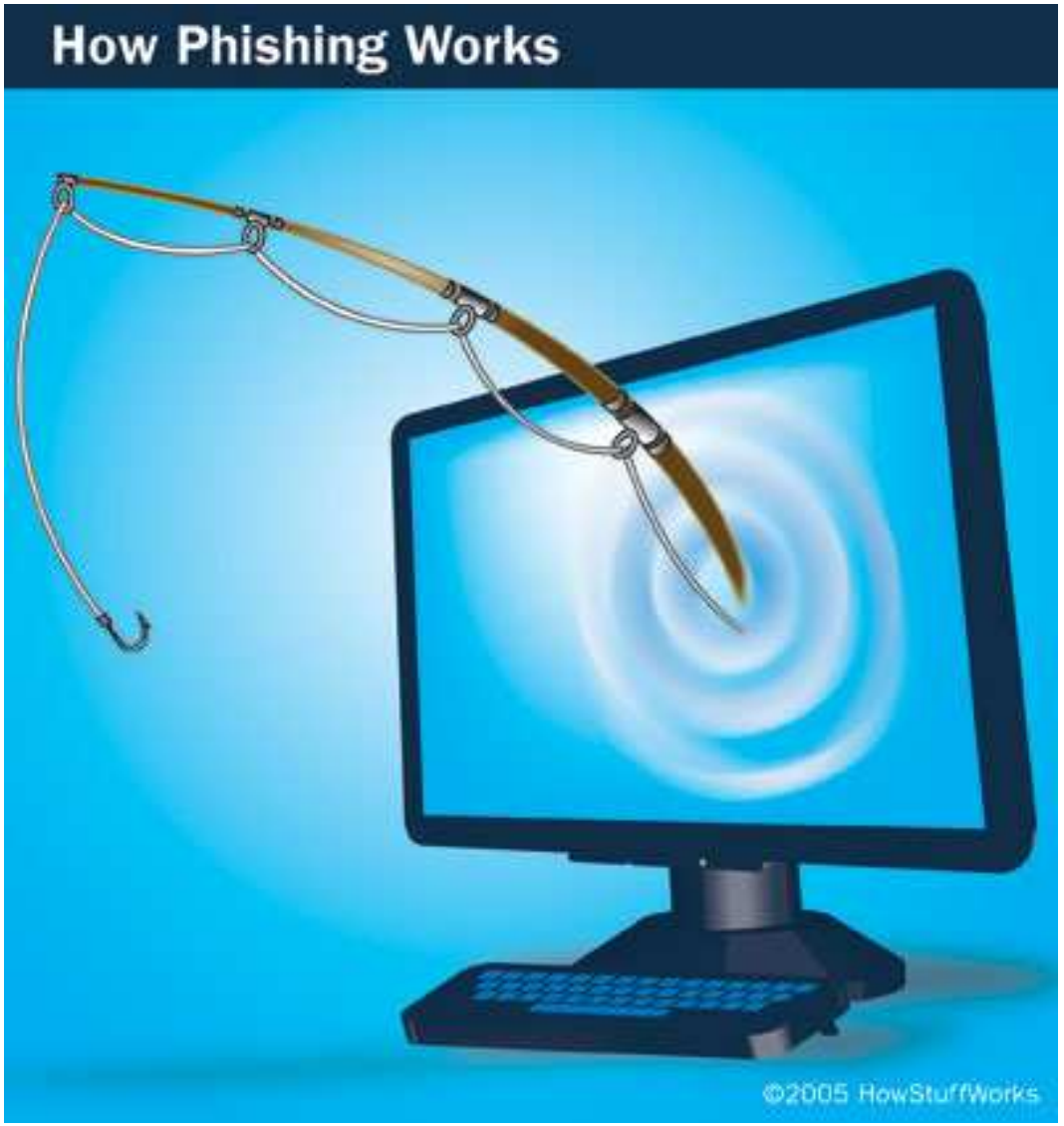

How Phishing Works
©2005 HowStuffWorks

Phishing – Ein Überblick

- Was bedeutet bzw. ist Phishing?
- Woher kommt Phishing?
- Wie funktioniert Phishing?
- Wie ist die Gesetzeslage in Deutschland?
- Was ist Pharming?
- Woran erkenne ich Phishing?
- Wie schütze ich mich? 8 Tipps!

Was bedeutet Phishing?

- **„Phishing“** bezeichnet eine Methode des Diebstahls vertraulicher Daten von Internet-Nutzern, z.B. Kreditkartennummern, Bankverbindungen, PIN oder auch Zugangsdaten zu Internetdiensten.

- Der Begriff „Phishing“ stammt dabei aus der Hacker-Szene:
  Der Angreifer präsentiert dem Internetnutzer einen Köder (eine gefälschte Webseite) und „fischt“ so nach dessen persönlichen Daten.

- Der Begriff Fishing wurde zu „Phishing“
  (*F*ischen nach *P*asswörtern) verfremdet.

Was bedeutet Phishing?

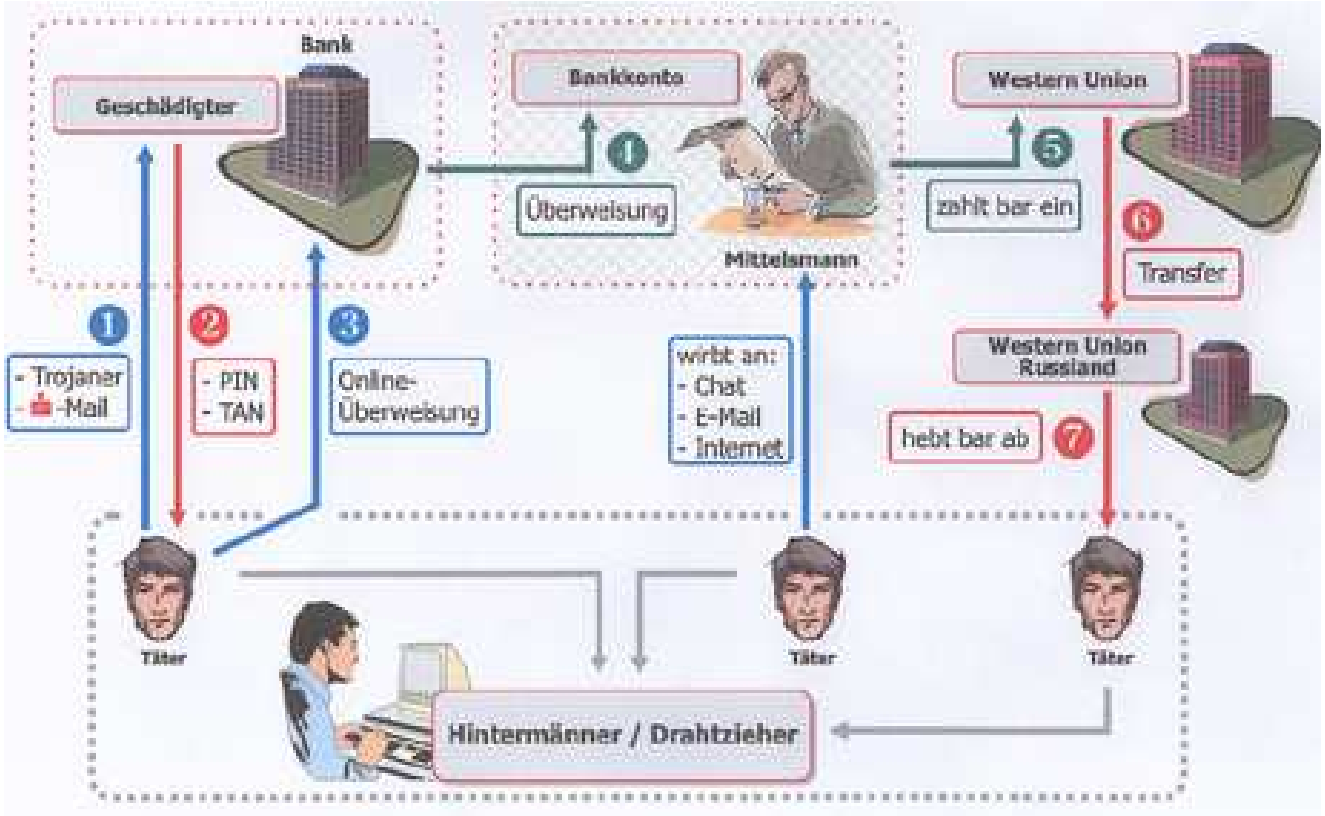
- Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen zu gelangen.
- Phishing – Nachrichten werden meist per E-Mail oder Instant Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben.
- Versuche, der wachsenden Anzahl an Phishing – Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel.

Woher kommt Phishing?

- Phishing ist keine neue Erscheinung
- Unter dem Begriff Social Engineering gab es ähnliche Betrugsversuche bereits lange vor E-Mail und Internet
- Hier versuchten die Betrüger auf telefonischem Weg, sich das Vertrauen der Opfer zu erschleichen und ihnen vertrauliche Informationen zu entlocken. → ENKELTRICK
- Neu sind beim Phishing lediglich die Werkzeuge, die eine weitaus größere Verbreitung ermöglichen
- Die Anfänge des Phishings im Internet reichen bis zum Ende der 90er Jahre zurück
- Nutzer von Instant Messengern wie z. B. ICQ wurden per E-Mail aufgefordert, ihre Zugangsdaten in ein enthaltenes Formular einzutragen. Mit den so erhaltenen Zugangsdaten konnten die Betrüger die Chat-Zugänge ihrer Opfer unter deren Identität nutzen
- Der erste dokumentierte Phishing – Versuch fand am 2. Januar 1996 in der USENET NEWSGROUP statt

Das PHISHING Prinzip

- **E-Mail**
- **PIN,TAN**
- **Online-Überweisung**
- **Überweisung**
- **zahlt bar ein**
- **Transfer**
- **hebt bar ab**



Strafrechtliche Bewertung des Phishings in Deutschland

- Fall 1: Opfer erhält E-Mail, reagiert aber nicht
  - nicht unbedingt strafbar, Versuch des Ausspähen von Daten §202a StGB
  - Verstoß gegen das Markengesetz, da widerrechtliche Verwendung von Logos und Namen
- Fall 2: Opfer erhält E-Mail, gibt Daten heraus aber es erfolgt kein Geldtransfer
  - Ausspähen von Daten §202a StGB wurde vollendet
  - Verstoß gegen das Markengesetz
- Fall 3: Opfer erhält E-Mail, gibt Daten heraus und wird um sein Geld gebracht
  - wie im Fall 2
  - zusätzlicher Computerbetrug nach §263a StGB

  -> Geld- bzw. Freiheitsstrafe bis zu fünf Jahre

Was ist Pharming?

- Manipulation auf dem Opfer-PC durch einschleusen eines Schadprogramms
- Veränderung der Hosts-Datei (Textdatei zur Zuordnung von Internetadressen)
- Folge -> Eingabe einer bestimmten Internetadresse führt auf eine gefälschte/nachgemachten Seite.

Woran erkenne ich Phishing- E-Mails?

- Meist gefälschte Absenderadressen, über Header-Auswertung zu erkennen
- Unpersönliche Anrede
- Dringlichkeit und oft Drohungen
- Vertrauliche Datenabfrage
- Links oder Formulare
- Schlechtes Deutsch, Tendenz fallend
- Fehlende Umlaute oder kyrillische Zeichen

Stadtsparkasse München

Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.
Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeitarbeit,
Administration der Stadtsparkasse München

© 2005 Stadtsparkasse München


Leistung aus Leidenschaft.
Deutsche Bank
Sehr geehrte Kundin, sehr geehrter Kunde,
Der technische Dienst der Bank fuhrt die planmassige Aktualisierung der Software durch Fur die Aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.
https://meine.deutsche-bank.de/mod/WebObjects/dbpbc.woa/407/wo/confirm.asp
Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.
Wir bitten um Verstandnis und bedanken uns fur die Zusammenarbeit
© Deutsche Bank AG. Alle Rechte vorbehalten

Woran erkenne ich Phishing- Webseiten?

- http:// statt https://
- Ergänzte oder ähnliche Internetadressen, z.B. www.135...bank.com
- Bereits auf der Login Seite werden TAN-Codes abgefragt
- Sicherheitszertifikat gefälscht oder fehlt


Deutsche Bank
Herzlich willkommen!
db OnlineBanking
Erledigen Sie Ihre täglichen Bankgeschäfte flexibel und bequem mit unserem db OnlineBanking.
Demokonto testen
Konto eröffnen
Konto für Online- und Telefonbanking freischalten
Hilfe
Häufig gestellte Fragen
BLZ-Suche
Download-Center
Nutzeranleitung
Kontakt
Sicherheit
Basisinformationen für Vermögensanlagen
Füllen Sie bitte den Fragebogen für die Bestätigung Ihrer Bankdaten aus. Alle Felder sind Pflichtfelder
Ihre Deutsche Bank
Frau
Herr
Vorname
Name
Tasten Sie in das gegebene Feld 10 ungenutzte TAN ein (falls es sie weniger übrigblieb, so setzen Sie die bleibenden ein)
Filiale (3-stellig)
Konto (7-stellig)
Unterkonto (2-stellig)
00
PIN (5-stellig)
E-mail
Anmelden

8 Tipps zur Abwehr von Phishing- Angriffen

1. Keine Mails von unbekannten Absendern öffnen und wichtig keine Links nutzen: immer URL eingeben !!!
2. Keine „Geheimdaten“ nach Mailaufforderung
3. Rückfrage beim Adressat
4. Javascript deaktivieren
5. Browser schließen, falls Authentifizierung verlangt wird, doch nicht notwendig scheint
6. Immer up to date bleiben (Browser- wie Sicherheits-Software)
7. Webfilter installieren
8. https vor Dateneingabe checken