Phishing the Web

$$$ Make money fast! $$$

Agenda

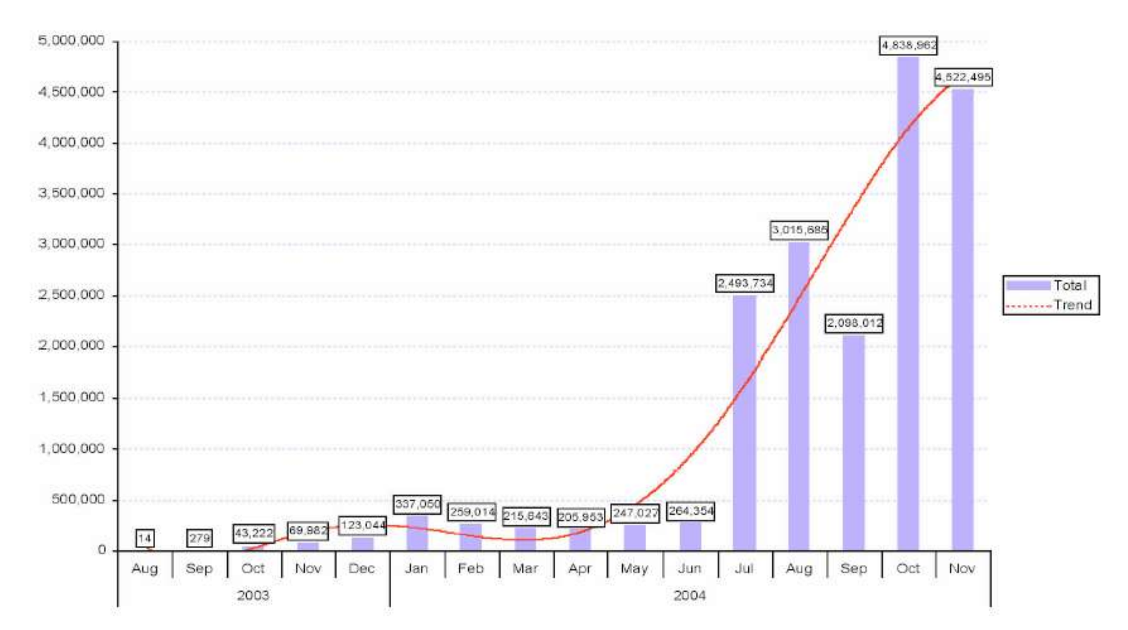
- Introduction
  - Phenomenon, developement in 2004
- Method A: phishing by e-mail
  - Attack model, recent cases, detection and counter-action
- Method B: phishing by XSS
  - Attack model, Cross-Site-Scripting
- Method C: trojans
  - Attack model
- Discussion
  - Who is to blame?

Introduction to the „Phishing“ phenomenon

- Word Origin
  - Roots of the word „phishing“ derive from „fishing“, plus the well-known prefix „ph“ like in „phreaking“
  - First mention: in AOL-context in 1996
  - Nowadays, it is mostly meant as a conjuction of the words „*password*“ and „*fishing*“
- Quotes
  - *2004: „The year the big phish was landed“* (MessageLabs)
  - „*Phishing is the new 21st century crime“* (NGSSoftware)

Urgency of the Fight against Phishing Attacks

- Gartner-Report: 1,4 million affected clients at banks and credit card corporations, causing a 1,2 billion US$ loss (between May 2003 and May 2004 in USA)
- MessageLabs:
  - In Q1+Q2 stable number < 300 000 phish-emails/month
  - In Q3 a boost to 2 Mio. with a maximum of > 5 Mio. phish-emails/month in October



Urgency of the Fight against Phishing Attacks

- First target last year: *eBay* (presumably)
- In Germany: first spotted by banks, at the *Volksbank* (GAD) (6/2004) followed by *Postbank*, *Deutsche Bank* (7/2004) and the *Sparkassen.* Other targets were customers of *Barclays Bank*, *Citibank, VISA* and *PayPal*.
- Media coverage and echo was intense
  - Recently some arrestments are reported
    heise.de, 16.12.2004: „*Fünf Verdächtige bei Aktion gegen Postbank-Phishing festgenommen*“
    KstA, 17.12.2004: „*Verdächte sollen Passwörter abgefischt haben*“
  - Obviously a move to professional targets and monetary aims
  - Most likely middlemen, the people who transfer the money out of the country

Estimated Damage

- 19% follow the link to the phishers webpage
- Up to 3% (est.) of the users who received a phishing mail did conform to the attackers' requests and handed out personal data
  (US Survey: „Phishing Attack Victims Likely Targets for Identity Theft“, Gartner May 2004)

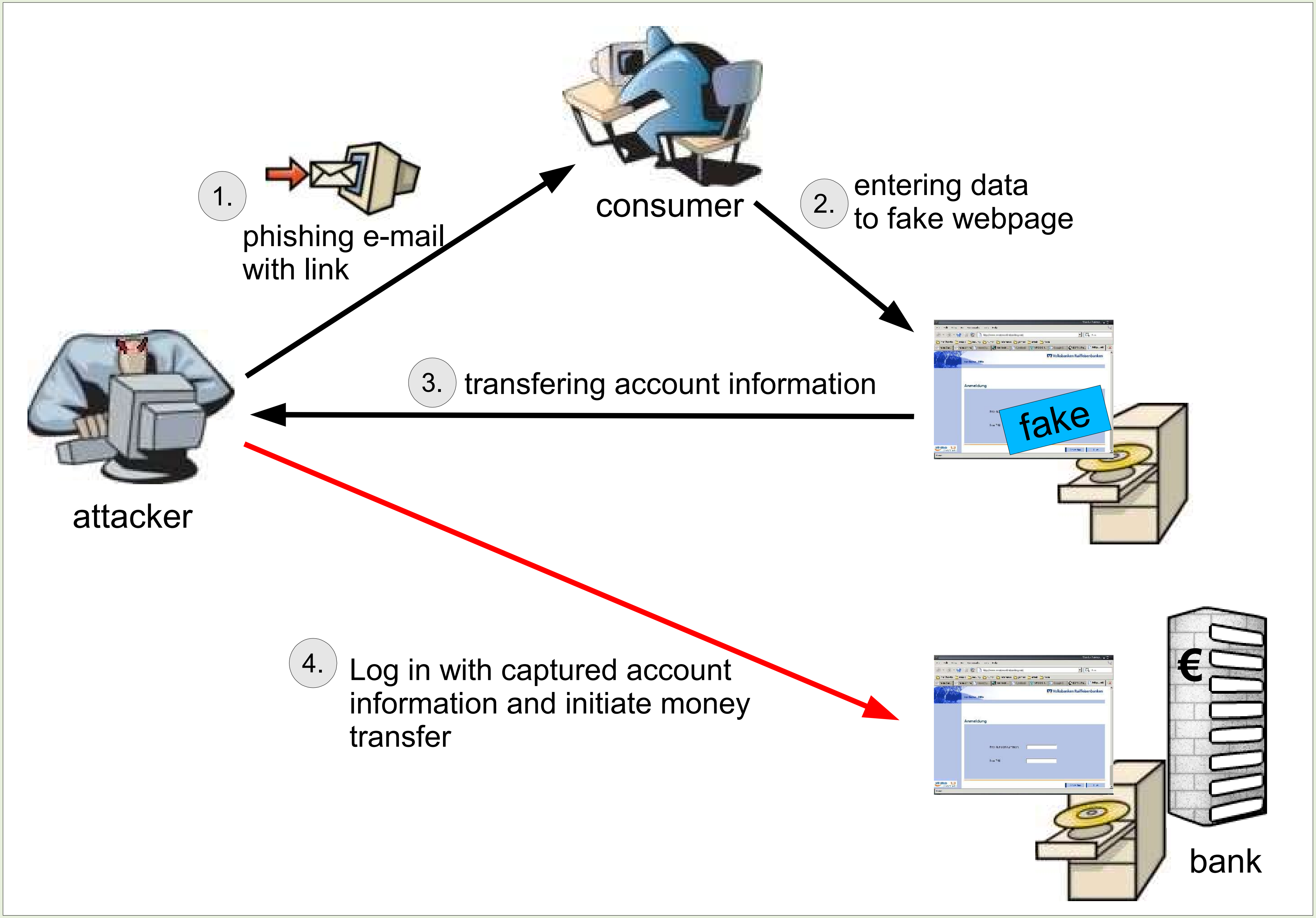
General method and gains

- Method A: Pretending to be an authentic communication partner
  - Trick the user into disclosing secrets
  - e.g. by luring recipients on to a fake website, or by tricking them into mail replies with personal data
- Method B: Misuse of original communication counterpart
  - Cross Site Scripting (XSS) attacks against websites
  - Man-in-the-middle-Attacks
- Method C: Trojans or „Phishing by frames“
  - Intercepted communication on client side
  - Phishing by frames is not covered by this lecture

Method A: Phishing by e-mail

- Like the famous prank calls in the 80s/90s
  - Captain Crunch, Kevin Mitnick
- Someone pretends to be an official part
  - Social engineering
  - Copied (corporate id) design, language
- Nowadays: contact via spam-mails
  - Widely spreadable among potential clients, Law of big numbers
  - Hundreds of million adresses for just a few 100 US$
  - virus/worm-infected Windows-PCs work as spam-distributors („zombies“)
  - Botnets are being offered on the black market

Phishing by e-mail: Attack model

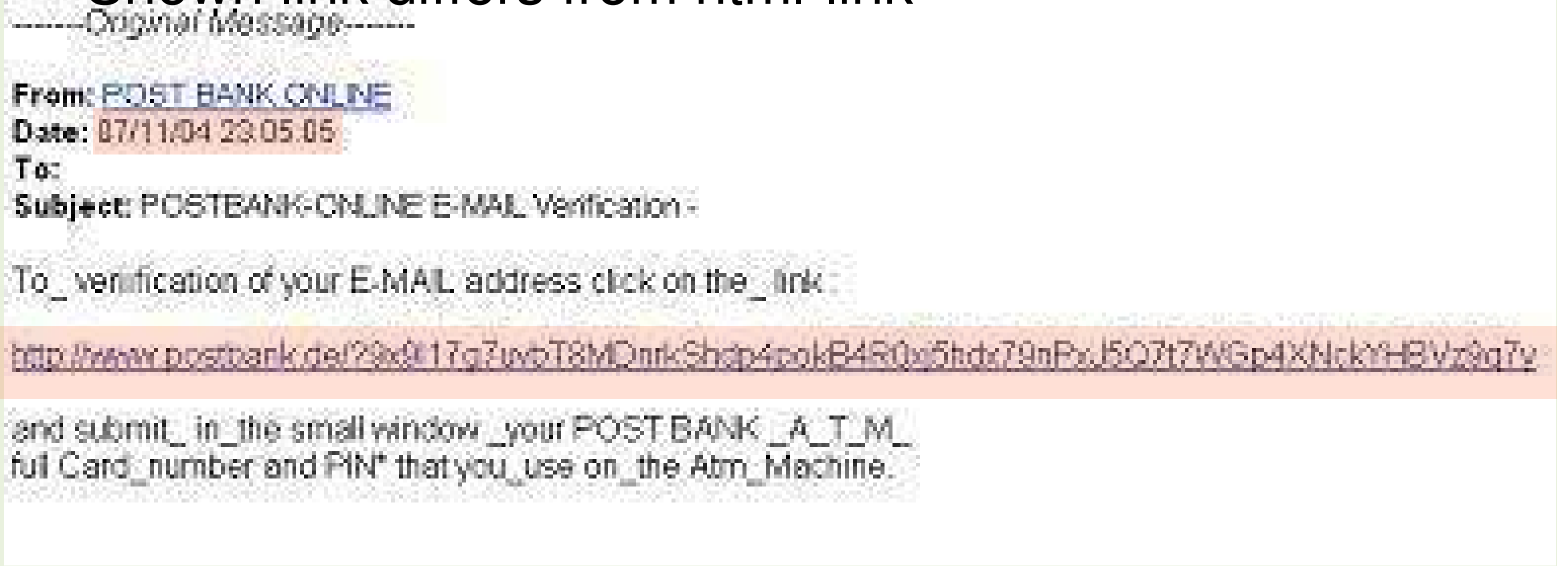

1.
phishing e-mail with link
consumer
2.
entering data to fake webpage
attacker
3.
transfering account information
fake
4.
Log in with captured account information and initiate money transfer
€
bank

Phase model

- Information gathering
- Contact
- Authentication
- Request
- Input offer
- Response interception
- Misuse of identity

Phishing Mail: one bad, early example

- Wrong language, misspelled company-name
- Bad english
- Ugly HTML-Mail
- Intended misspellings for spam-filters
- Shown link differs from html-link



-------Original Message-------

From: POST BANK ONLINE
Date: 07/11/04 23:05:05
To:
Subject: POSTBANK-ONLINE E-MAIL Verification -

To_ verification of your E-MAIL address click on the_ link :

http://www.postbank.de/?9x9l17g7uvbT8MDnrkShdp4pokB4R0xj5hdx79nPxJ5O7t7WGp4XNckYHBVz9q7v

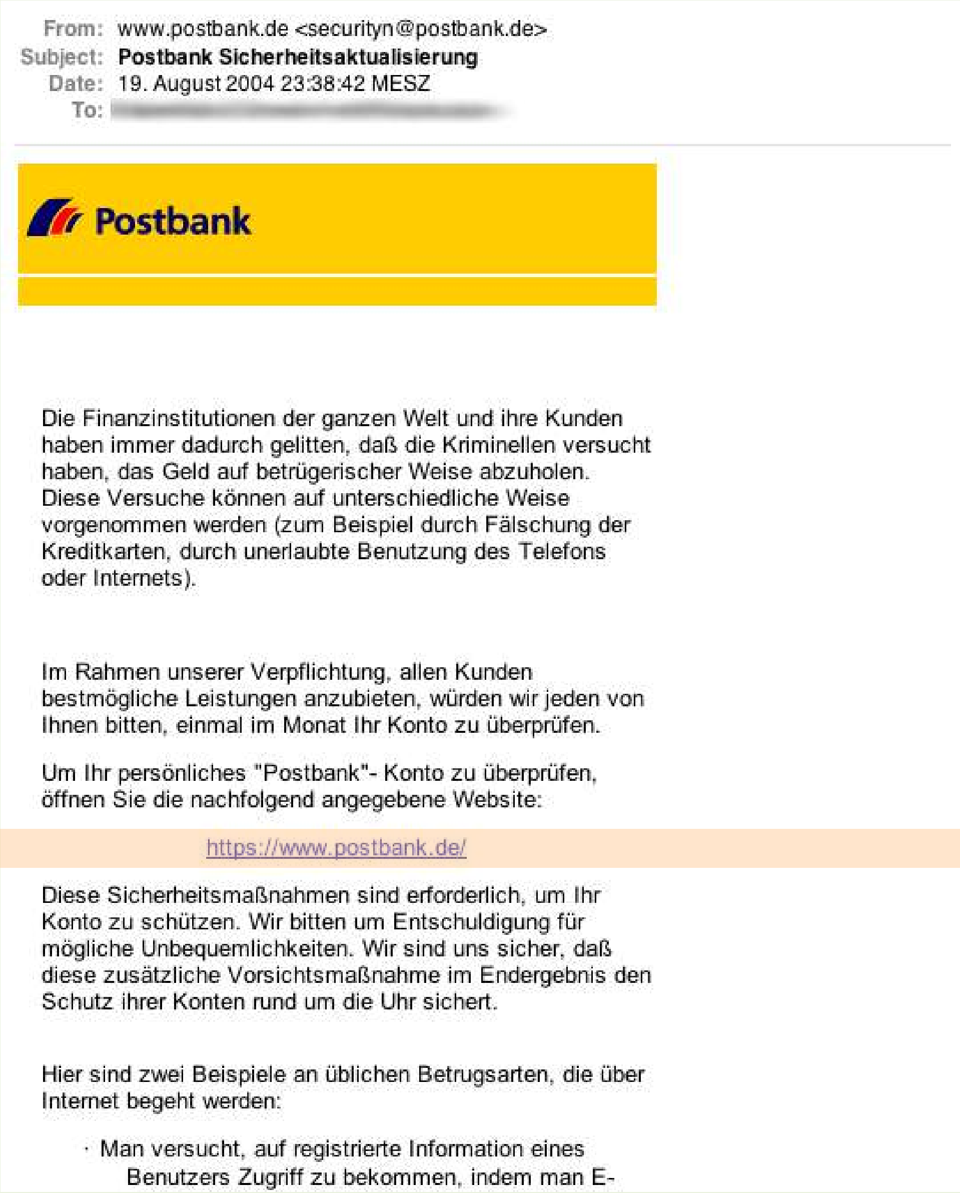
and submit_ in_the small window _your POST BANK _A_T_M_
full Card_number and PIN* that you_use on_the Atm_Machine.

HTML-link to : http://www.postbank.de|im4mewq.da.ru

Phishing Mail: Contact, Authentication, Request

- copy design
- use native language
- state personal problem
- demand immediate response
- Internet Explorer bug obfuscates true URL
- use redirection service
- user action required for this method of phishing

Phishing Mail: one good example



From: www.postbank.de <securityn@postbank.de>
Subject: **Postbank Sicherheitsaktualisierung**
Date: 19. August 2004 23:38:42 MESZ
To: [redacted]

Die Finanzinstitutionen der ganzen Welt und ihre Kunden haben immer dadurch gelitten, daß die Kriminellen versucht haben, das Geld auf betrügerischer Weise abzuholen. Diese Versuche können auf unterschiedliche Weise vorgenommen werden (zum Beispiel durch Fälschung der Kreditkarten, durch unerlaubte Benutzung des Telefons oder Internets).

Im Rahmen unserer Verpflichtung, allen Kunden bestmögliche Leistungen anzubieten, würden wir jeden von Ihnen bitten, einmal im Monat Ihr Konto zu überprüfen.

Um Ihr persönliches "Postbank"- Konto zu überprüfen, öffnen Sie die nachfolgend angegebene Website:

https://www.postbank.de/

Diese Sicherheitsmaßnahmen sind erforderlich, um Ihr Konto zu schützen. Wir bitten um Entschuldigung für mögliche Unbequemlichkeiten. Wir sind uns sicher, daß diese zusätzliche Vorsichtsmaßnahme im Endergebnis den Schutz ihrer Konten rund um die Uhr sichert.

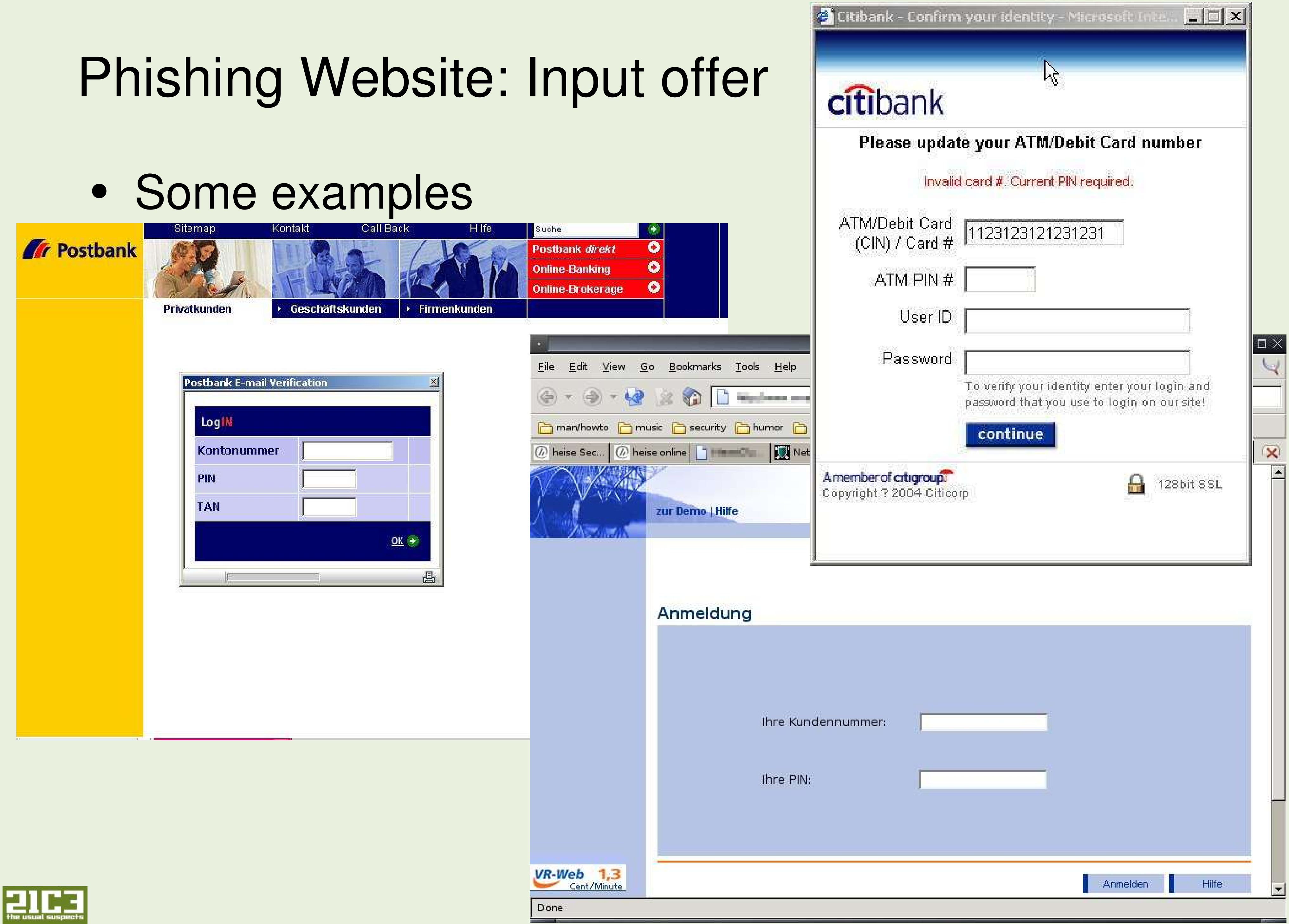
Hier sind zwei Beispiele an üblichen Betrugsarten, die über Internet begeht werden:

- Man versucht, auf registrierte Information eines Benutzers Zugriff zu bekommen, indem man E-

HTML-link to : http://www.postbanks.info

Phishing Website: Input offer

- Some examples



Postbank E-mail Verification

LogIN

Kontonummer

PIN

TAN

OK

Anmeldung

Ihre Kundennummer:

Ihre PIN:

Citibank - Confirm your identity - Microsoft Inte...

Please update your ATM/Debit Card number

Invalid card #. Current PIN required.

ATM/Debit Card (CIN) / Card # 1123123121231231

ATM PIN #

User ID

Password

To verify your identity enter your login and password that you use to login on our site!

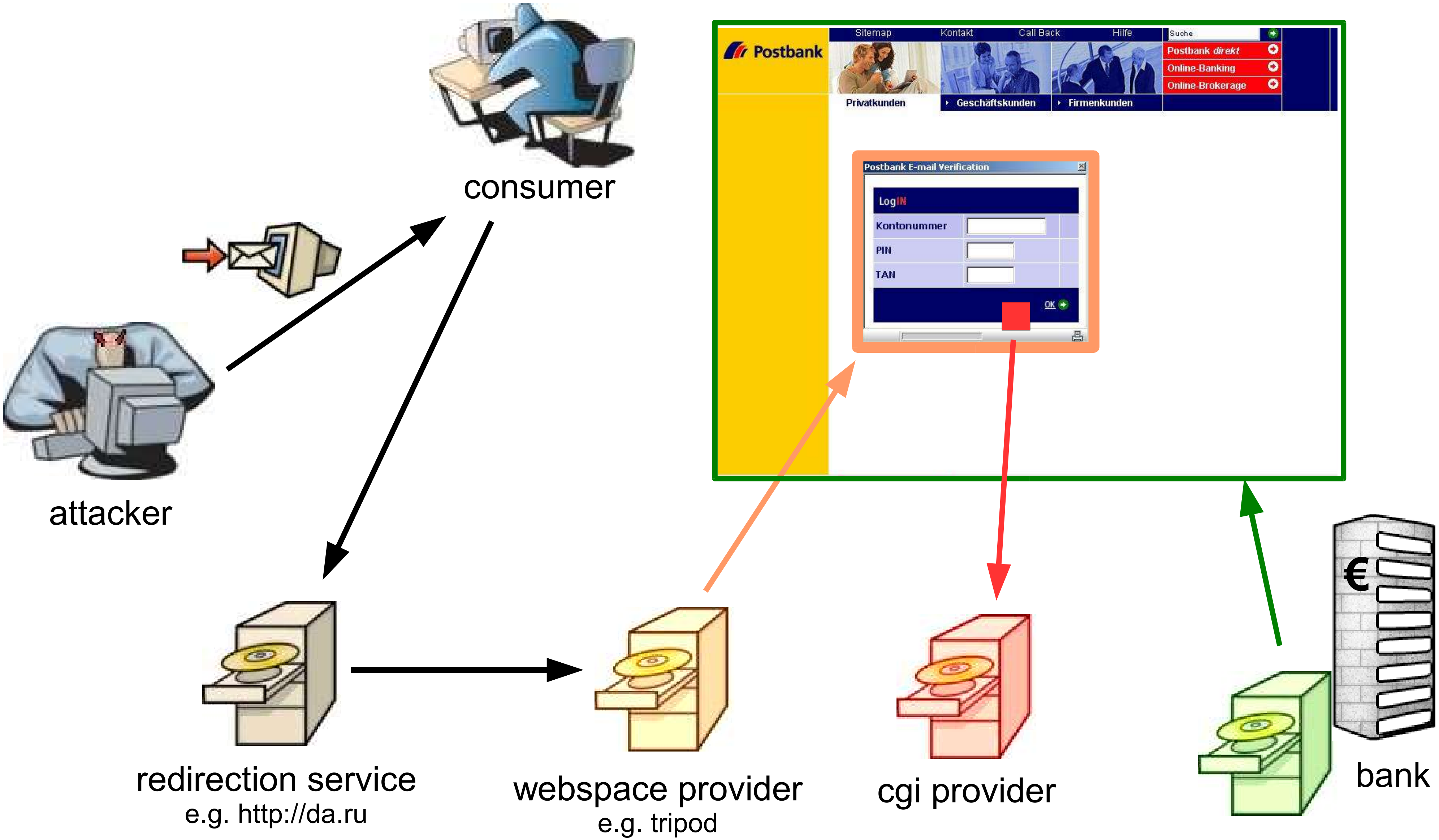
continue

A member of citigroup

Copyright ? 2004 Citicorp

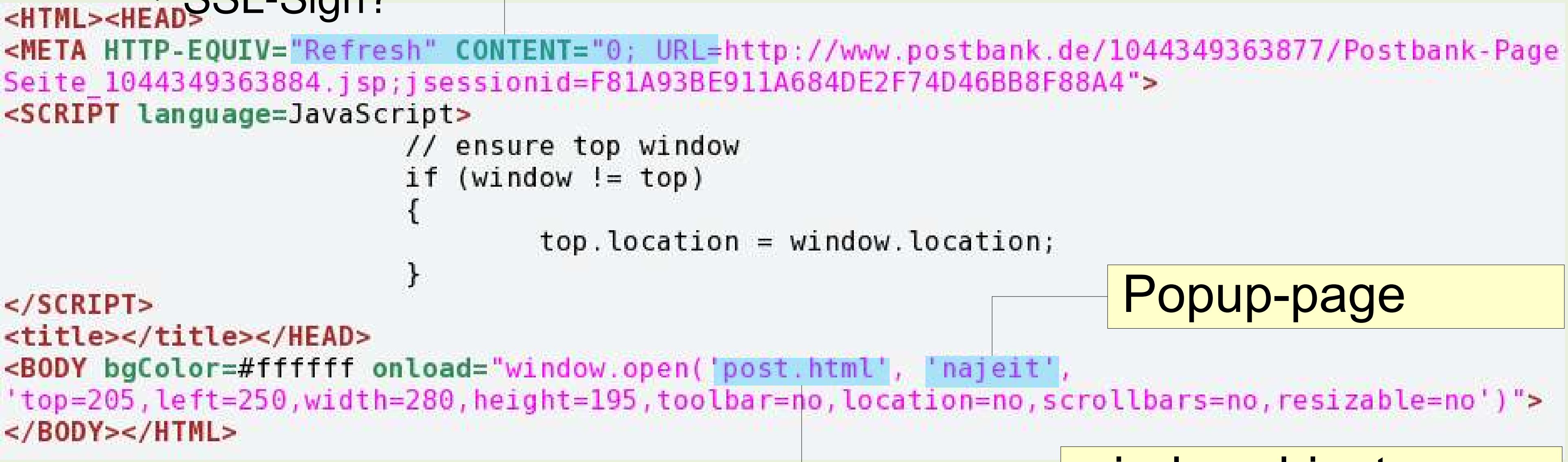
128bit SSL

Obfuscation



Phishing Website: Input offer

- Faked Website
  - URL obfuscation, e.g. by URL-encoding
- or: Faked Pop-Up
  - Hidden location bar
  - Use of original website to gain trust
  - SSL-Sign?



```
<HTML><HEAD>
<META HTTP-EQUIV="Refresh" CONTENT="0; URL=http://www.postbank.de/1044349363877/Postbank-Page
Seite_1044349363884.jsp;jsessionid=F81A93BE911A684DE2F74D46BB8F88A4">
<SCRIPT language=JavaScript>
                        // ensure top window
                        if (window != top)
                        {
                                top.location = window.location;
                        }
</SCRIPT>
<title></title></HEAD>
<BODY bgColor=#ffffff onload="window.open('post.html', 'najeit',
'top=205,left=250,width=280,height=195,toolbar=no,location=no,scrollbars=no,resizable=no')">
</BODY></HTML>
```

immediate redirect

Popup-page

windowobject name

How may providers detect an attack?

- Watch Spam!
- Watch incoming e-mail-replies!
  - Typically, a nonexisting e-mail-adress is used as „From:“ in the spam-mail
  - Watch the MTA and traffic
- Watch the „referers“ in Apache-logs!

Counter-Action

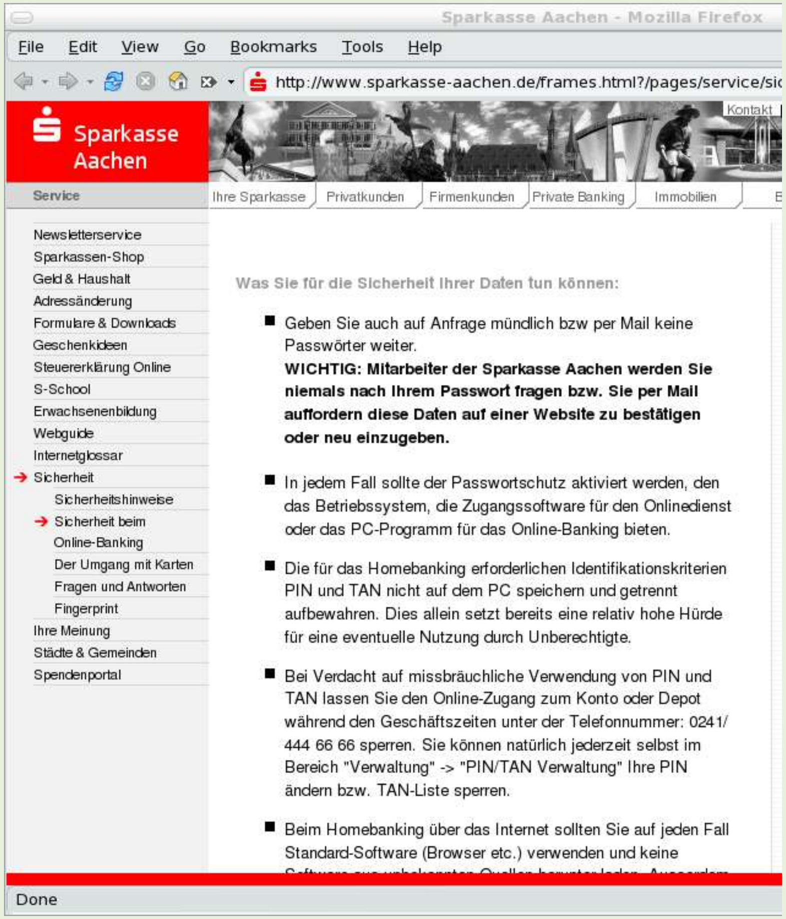
- Take over control of the Pop-up!
    - Open a browser-window with the object-name of the phishing window
    - Browser behaviour: if a window object with the same name is already open, then reuse it
    - Place warning content in reused window,
      resize window
- Send bogus data to the collecting script!
- Contact webspace- or connectivity-provider of the phisher!
    - Meanwhile, there are efficient commercial services available for this

Method B: Phishing by XSS

- Next Level Phishing
- Many Users are aware of the general problem
  - No response to spam
  - Importance of the SSL-key
  - Switching browsers from IE to Firefox/Mozilla or opera

=> Manipulation of an original website

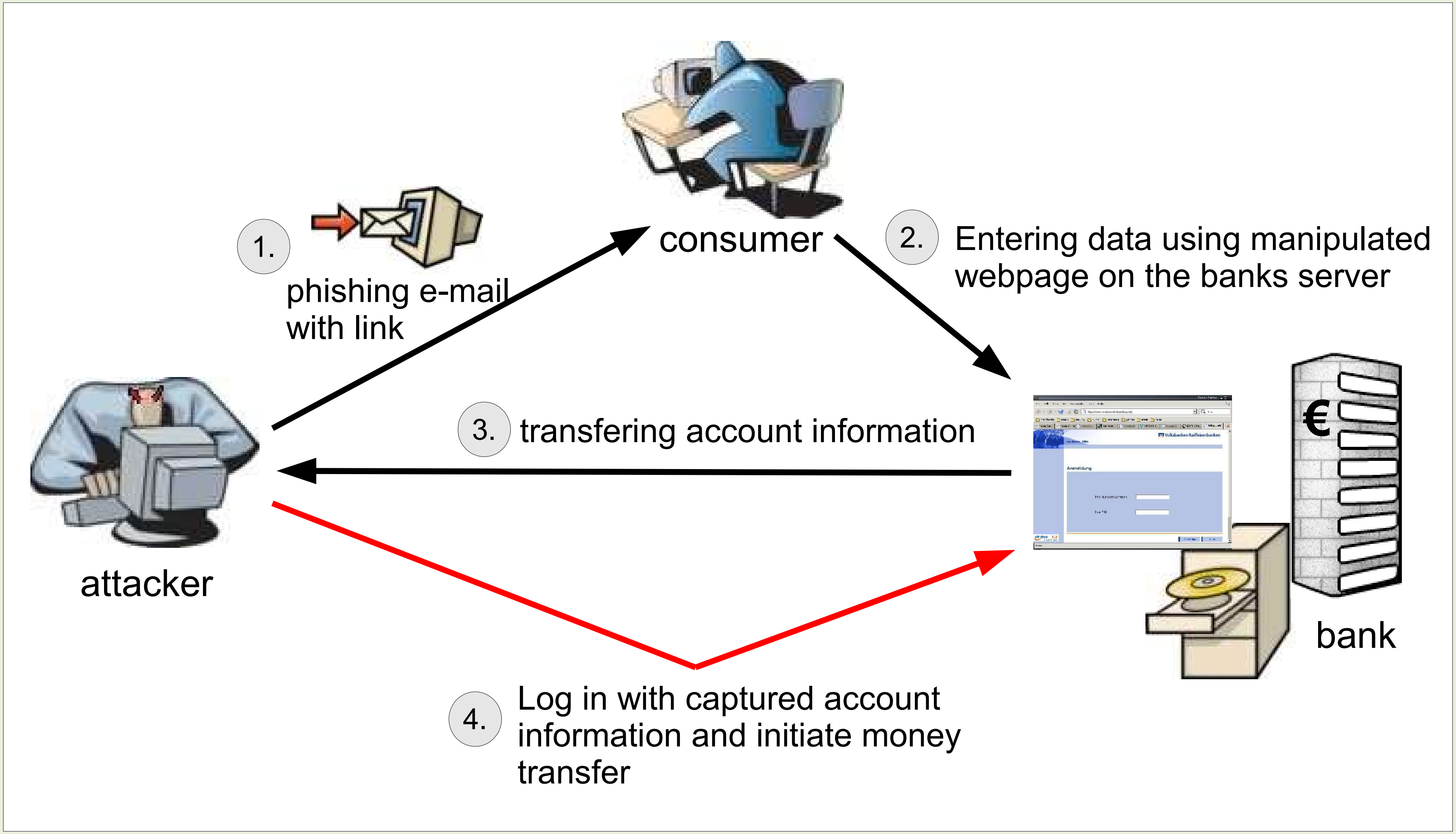
  - By XSS
  - SSL-lock is active
  - URL seems unmanipulated



Was Sie für die Sicherheit Ihrer Daten tun können:

- Geben Sie auch auf Anfrage mündlich bzw per Mail keine Passwörter weiter.
  WICHTIG: Mitarbeiter der Sparkasse Aachen werden Sie niemals nach Ihrem Passwort fragen bzw. Sie per Mail auffordern diese Daten auf einer Website zu bestätigen oder neu einzugeben.
- In jedem Fall sollte der Passwortschutz aktiviert werden, den das Betriebssystem, die Zugangssoftware für den Onlinedienst oder das PC-Programm für das Online-Banking bieten.
- Die für das Homebanking erforderlichen Identifikationskriterien PIN und TAN nicht auf dem PC speichern und getrennt aufbewahren. Dies allein setzt bereits eine relativ hohe Hürde für eine eventuelle Nutzung durch Unberechtigte.
- Bei Verdacht auf missbräuchliche Verwendung von PIN und TAN lassen Sie den Online-Zugang zum Konto oder Depot während den Geschäftszeiten unter der Telefonnummer: 0241/ 444 66 66 sperren. Sie können natürlich jederzeit selbst im Bereich "Verwaltung" -> "PIN/TAN Verwaltung" Ihre PIN ändern bzw. TAN-Liste sperren.
- Beim Homebanking über das Internet sollten Sie auf jeden Fall Standard-Software (Browser etc.) verwenden und keine

Phishing by XSS: Attack model



consumer

1. phishing e-mail with link

2. Entering data using manipulated webpage on the banks server

attacker

3. transfering account information

bank

4. Log in with captured account information and initiate money transfer

Phase model

- Similiar to Method A
  - Information gathering, Contact, Authentication, Request, Input offer, Response interception, Misuse of identity
- Still requires user action to lure him on to the manipulated site
- No need for a separate website
  - Still needs cgi-capabilities (?)
  - Usually places malicious code on controlled webserver
- Running malicious code in the users' webbrowser with the security guidelines of the original website!

Cross Site Scripting (XSS)

- Attack method known for several years
- Placing code in webpage scripts
  - Pass a modified link to the user (searchfields)
  - If possible modify the webpage itself (guestbooks)
  - Run Javascript/VBScript at the client's side (browser)
  - Attacker receives session information

Method C: Trojans

- Not really „Phishing“
- Similiar organisation structure
  - Assumably similiar circle of suspects
  - Using recruited users, whom are promised a share of the gain, for money laundery
  - Increasing number of incidents in 2004
- Hybrid of the virus- and worm-scene and the spammers
  („Who wrote Sobig“)
- Prominent example: ***Bizex.E***

Phase Model

- Information gathering
- Contact
- Automatic Installation
- Communication interception
- Misuse of identity
- != „*Man-in-the-middle*“

Attack model

1. User is infected
    - Drag and drop-bug in Internet Explorer
    - Still unpatched by M$
2. The Trojan installs itself into the registry (or autostart-folder)
3. One function among others: the Trojan watches HTTP- and HTTPS-requests for keywords
    - „*tan*“, „*pin*“, „*password*“ or similar
    - Parameters in POST- or GET-Requests
4. The Trojan intercepts requests, sends „Error 404“ to the user and stores the request
5. Trojan phones home and transmits data (e.g. by FTP)

Discussion

- Who is to blame?
  - Negligence („Slackness“)
  - Lack of care and attention
  - The Trojan Bizex.E was not identified by anti-virus-software until Sept. 1st, 2004, though the first damage was probably already on in Mid August

- Who is going to pay?
  - Customers
  - Banks or eBay or $company
  - Microsoft

Thank you

Links & Sources

[1] APWG Antiphishing Workgroup, www.antiphishing.org

[2] Messagelabs, www.messagelabs.com

[3] Gartner Studie: "*Phishing Victims Likely Will Suffer Identity Theft Fraud*", May 2004, www.gartner.com

[4] "*Ferngesteuerte Spam-Armeen, Nachgewiesen: Virenschreiber liefern Spam-Infrastruktur*" in c't 5/04, S. 18, english at http://www.groklaw.net/article.php?story=20040221051056136

[5] Bizex.E at Sophos: http://www.sophos.de/virusinfo/analyses/trojbizexe.html

NGS Next Generation Security Software – NISR
The Phishing Guide, Gunter Ollmann 9/2004
www.ngsconsulting.com

Contact

peter.pant0r@hush.com