

openHPI course "Digital Identities
Identity thefts -
Social Engineering Attacks

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

What is Social Engineering?

Exploitation of human weaknesses, to provoke certain reactions

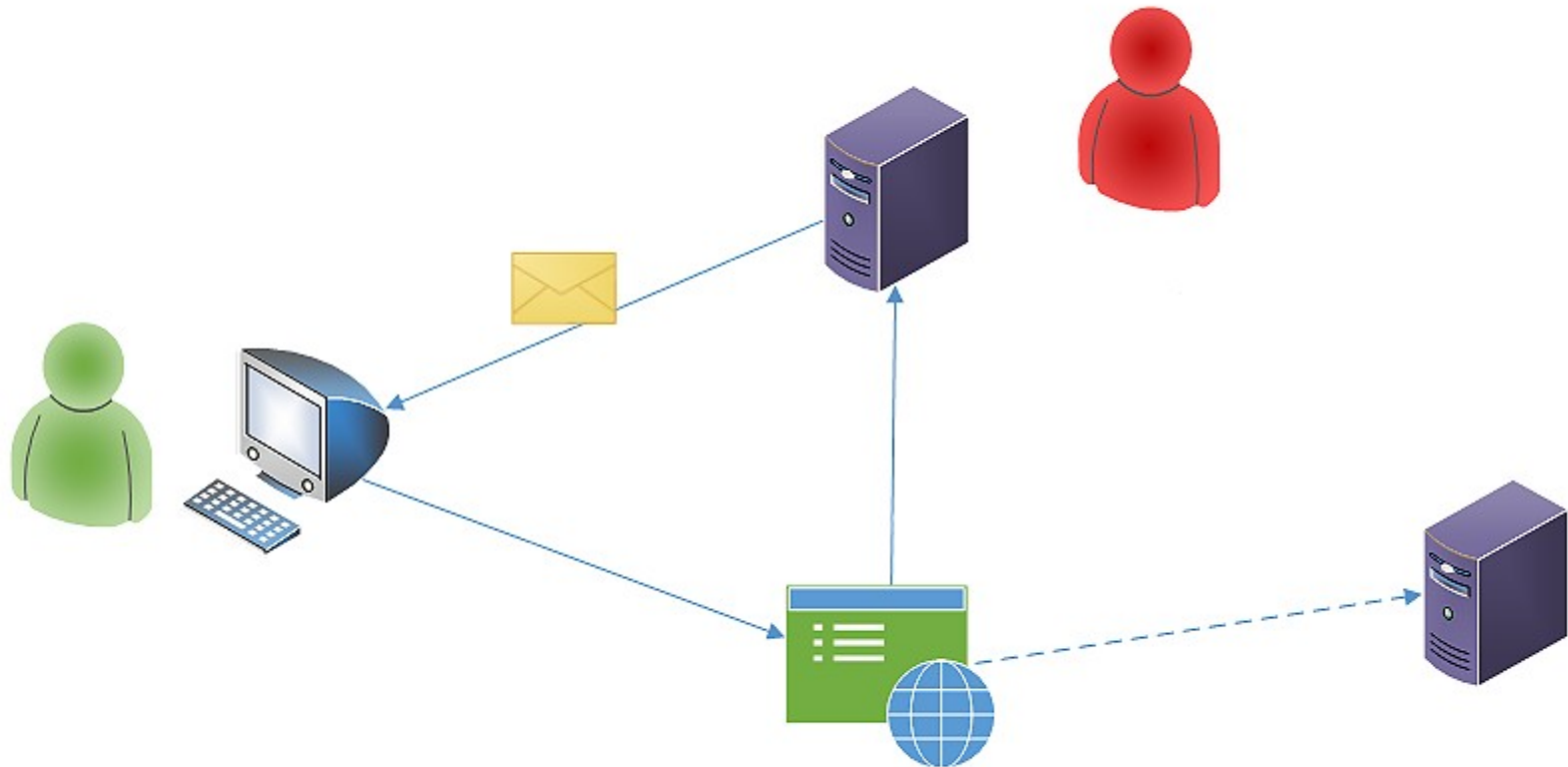
- Under false (e.g. stolen) identity, an attacker exploits human weaknesses (trust, fear, respect, helpfulness) of a victim
- Victim is made to do something that it wouldn't do under normal circumstances.
 - Publishing of information such as identity data
 - Grant access to a protected system / location
 - ...
- Most common method on the Internet: **phishing**

Phishing (1/2)

Technique for fraudulent acquisition of sensitive information

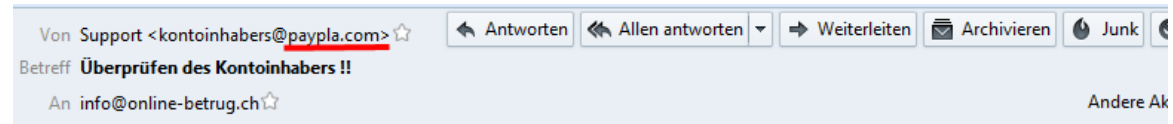
- Typical procedure: Sending fraudulent e-mails
 - Dispatch with trustworthy sender address, e.g. bank, company, authority, ...
 - Sender address is selected according to the information to be tricked into
 - Address can easily be forged or faked ("E-Mail Spoofing")
 - Exploitation of the confidence gained to evoke a desired reaction
 - release of data
 - Installation of malware

Phishing (2/2)



Phishing - Example (1/2)

- Sending an e-mail with a fake consignor
- Message originates allegedly by Bank (Paypal) and has a corresponding similar email address (paypla.com)
- **Objective:** To cause recipient to disclose his account details to reset account
- Phishing often recognizable by the many linguistic mistakes or lack of personal contact ("Good day Dear Customer")



- Ihr Kontozugang wurde für den folgenden Grund begrenzt: Wir haben während unserer geplanten Routineuntersuchung eine Unzulänglichkeit in Ihren Rechnungen gefunden.
- Wir haben den Zugang zu sensiblen Paypal Kontooption! en begrenzt bis Sie uns die verlangten Informationen zusenden.
- Wir verstehen dass begrenzter Kontozugang für Sie ein Problem darstellt, aber die Sicherheit Ihres Kontos ist unser hauptsächliches Interesse.

[Finden Sie aus wie Sie die Begrenzung aufheben können!](#)

Ihre Sicherheit ist unsere Priorität Mit freundlichen Grüßen, Paypal
 © 2012 Paypal
 Diese Email wurde info@online-betrug.ch gesendet
 Auf: Thu Sep 27, 2012 4:28 pm

Phishing - Example (2/2)

- Email forwards on website with prompt the account data
- Victim is invited, here all details via his account disclose



Restore Your Account

Please fill in all the details that are required to complete this verification process in order to restore your account.

NOTE: All fields are required

Please fill in all the fields.

Email Address:

PayPal Password:

Full Name:

Credit/Debit Card Number

Card Expiration Date

Source: <http://labs.m86security.com/>

Widely scattered phishing attacks

Conventional phishing attacks are relatively **easy to detect** today

- That's why phishing emails are spread very widely and randomly - with many millions of potential victims, a very low conversion rate is sufficient to achieve significant success.

Problems for attackers

- Internet users are well sensitized against common phishing scams by the media
- Phishing mails reach many recipients who are not even aware of it. and are therefore easy to see through.
- e.g. sender is bank where victim has no account at all

Personalized Phishing (1/2)

- Normal phishing not (anymore) suitable for
 - guaranteed information retrieval
 - Acquisition of sensitive information
- Attackers therefore switch to personalized phishing, the so-called **spear phishing**.
- For this purpose, attackers collect detailed information about his victim
 - helpful for pretending trustworthiness, e.g. using the identity of a person who knows victims and trusts them
 - Victim thinks email comes from fake sender because message contains information that only that sender knows
- The chances of success with this mesh are very high, but the effort for the attacker is of course much higher.

Personalized Phishing (2/2)

- Many attacks on the Internet are based on previous personalized phishing attacks
- Personalized phishing is therefore very dangerous and is aimed specifically at
 - high-ranking target persons, e.g. company bosses, politicians, high-ranking officials, celebrities, ...
 - Sensitive targets: Military, Business, Politics, Financial Industry...
 - Professional attackers, e.g. states, activists, organized crime

Other techniques of social engineering

■ **baiting**

- Exploitation of the curiosity/greed of victims
- Distribution of gifts with malicious secondary functions
 - e.g. USB sticks with malware, apps, ...

■ **pretexting**

- Pretending stories/lies that cause victims to release information or react in a particular way
- Presentation of the story under the pretence of an authority or an initiate

■ **reverse social engineering**

- Attacker contacts victim seeking help to gain trust

Protective measures (1/2)

- **Sensitisation of** users
 - through education, e.g. through our openHPI course
 - also by occasional tests with phishing emails
- **Verification of the identity of** the alleged counterparty
 - be better mistrusted and deported in case of doubt
- Use of **secure authentication**
 - e.g. via trustworthy certificates
- **Responsible handling of** personal information
 - What may be given to the outside world?

Protective measures (2/2)

Especially against phishing

- Check the sender's address - not the display name in the email program
- When requesting sensitive information, confirm the request with the service provider.
- If you follow a link, you have to enter the address in the browser address bar
 - common browsers often already warn about phishing sites

Summary:

social engineering attacks

■ **attack tactic**

- Attackers manipulate, exploit human weaknesses and build trust to induce certain behaviors in victims
- e.g. the release of sensitive information or the installation of malicious software
- Frequent procedures: Sending fraudulent e-mails or malicious calls

■ Special form: **Spear Phishing** (Personalized Phishing)

- Attacker focuses on a specific person and collects detailed information about his victim
- More elaborate, but more effective than "normal" phishing

Summary:

social engineering attacks

■ **attack tactic**

- Attackers manipulate, exploit human weaknesses and build trust to induce certain behaviors in victims
- e.g. the release of sensitive information or the installation of malicious software
- Frequent procedures: Sending fraudulent e-mails or malicious calls

■ Special form: **Spear Phishing** (Personalized Phishing)

- Attacker focuses on a specific person and collects detailed information about his victim
- More elaborate, but more effective than "normal" phishing