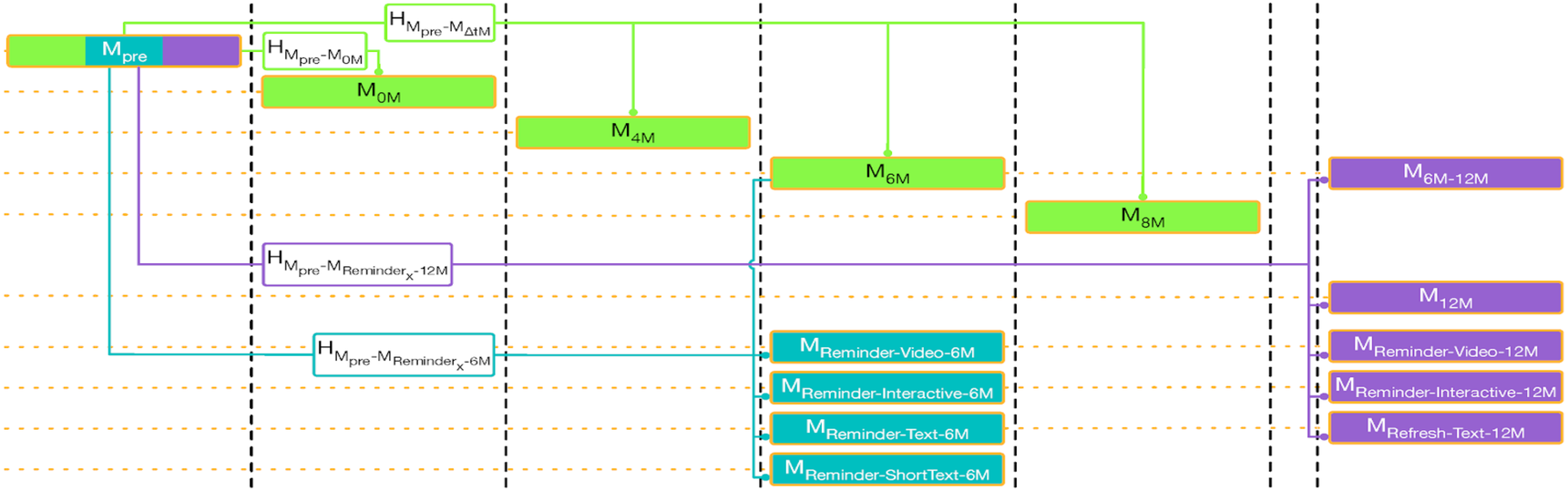
An investigation of phishing awareness and education over time: When and how to best remind users?

Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, Melanie Volkamer

COMPETENCE CENTER FOR APPLIED SECURITY TECHNOLOGY (KASTEL)
RESEARCH GROUP SECURITY · USABILITY · SOCIETY (SECUSO)

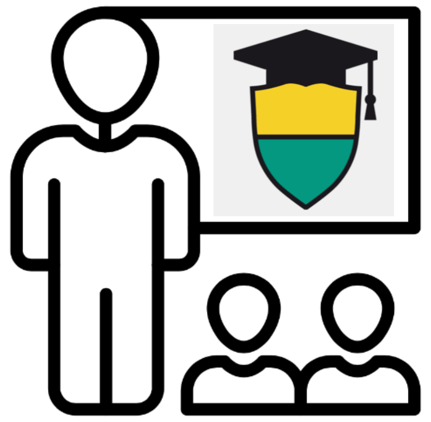


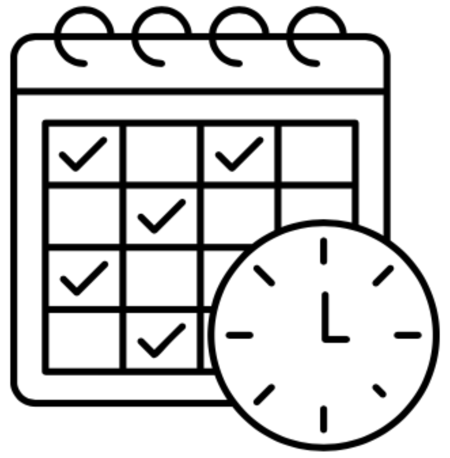
Contribution

Karlsruhe Institute of Technology

Longitudinal field-study

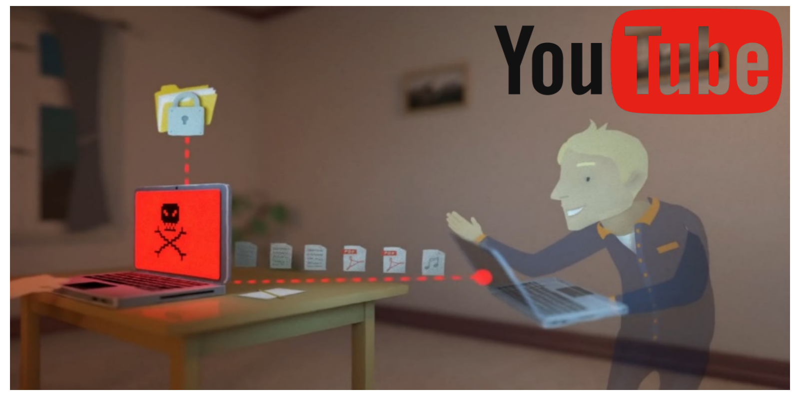
Systematically measure retention





Reminder measures

1.



2.

Fraudulent Mails

1. Rule: Check the sender and the contents of every mail for plausibility

2. Rule: Get familiar with where to find the real web address behind a link (e.g. for PCs or laptops in the tooltip or the status bar).

3. Rule: Identify the whois of the web address.

4. Rule: Check if the whois matchs with the supposed legit mail.

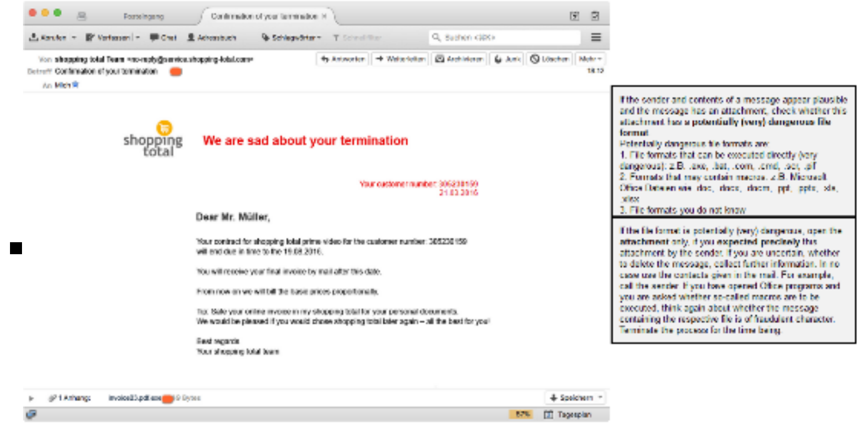
5. Rule: Check if the whois is written correctly

6. Rule: 6. If you cannot assess the whois clearly, collect further information, e.g. by searching the address in a search machine.

7. Rule: Check the file format of the attachment.

8. Rule: If you cannot clearly assess the attachment or if you are uncertain about expecting precisely this format by the sender, collect further information, e.g. by contacting the sender. In no case use the contacts given in the mail.

3.



4.

How to Detect Fraudulent and Phishing Mails

General Information

Criminals use various strategies to harm you. Popular attack strategies are

- the dissemination of malware to e.g. gain access to your devices or
- deception of the end users to obtain sensitive information (e.g. access data).

A widely used attack method is to send fraudulent messages to you that pretend to have a legitimate reason. Fraudulent messages may be received via different channels, e.g. as emails, SMS, via Messenger or social networks.
The contents of these messages may be dangerous in different ways:

Sensitive data: the messages ask you to return sensitive data, such as access data or documents worth protecting.

Money transfers/calls: messages ask you to transfer money or to call e.g. cooperation partners, supposed friends or business partners. In this way, criminals will get the money from by direct transfer or the money is debited with the telephone invoice.

Links: messages may contain one or several dangerous links. The fraud is aimed at making you click one of these links. These links will then lead you to e.g. a deceptively real-looking, but fraudulent website (also called phishing site) where you are supposed to log in. Alternatively, you are guided to a website that installs malware on your device.

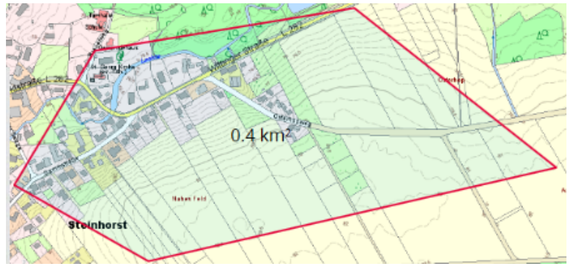
Attachments: messages contain one or several dangerous files (e.g. an attachment of an email). The criminals want to make you open the attachment. By opening or executing the file, malware is installed on your device.

Advertisements: messages may contain ads or other worthless contents (these messages are frequently called spams). The attack is aimed at making you buy something. In reality, the primary damage done is lost working time, because you look at the message, assess it, and delete it.

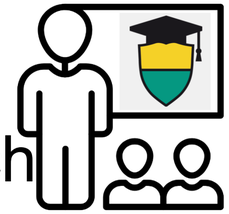
About the setting

State Office for Geoinformation and State Survey (SOGSS)

2,200 employees



Mandatory tutorial on phishing using a train-the-trainer approach



Optional participation in the study: 409 participants

Canova/Volkamer/Bergmann/Reinheimer: NoPhish app evaluation: lab and retention study. In *USEC 2015*
Neumann/Reinheimer/Volkamer: Don't be deceived: the message might be fake. In *TrutBus2017*
Stockhardt/ Reinheimer/Volkamer/Mayer/Kunz/Rack/Lehmann: Teaching phishing-security: which way is best?. In *IFIP Sec 2016*
…

Four Reminder Measures

Karlsruhe Institute of Technology

How to Detect Fraudulent and Phishing Mails

General Information

Criminals use various strategies to harm you. Popular attack strategies are

- the dissemination of malware to e.g. gain access to your devices or
- deception of the end users to obtain sensitive information (e.g. access data).

A widely used attack method is to send fraudulent messages to you that pretend to have a legitimate reason. Fraudulent messages may be received via different channels, e.g. as emails, SMS, via Messenger or social networks.
The contents of these messages may be dangerous in different ways:

Sensitive data: the messages ask you to return sensitive data, such as access data or documents worth protecting.

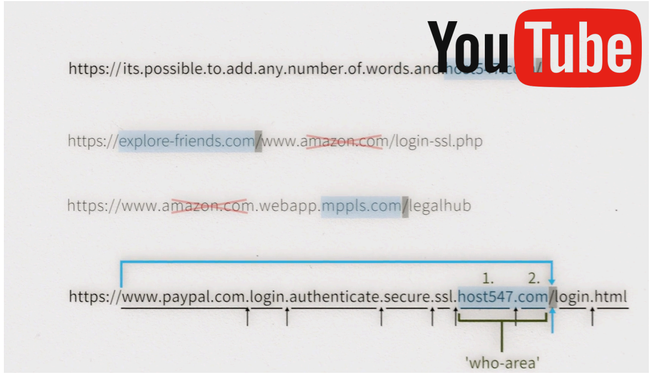
Money transfers/calls: messages ask you to transfer money or to call e.g. cooperation partners, supposed friends or business partners. In this way, criminals will get the money from by direct transfer or the money is debited with the telephone invoice.

Links: messages may contain one or several dangerous links. The fraud is aimed at making you click one of these links. These links will then lead you to e.g. a deceptively real-looking, but fraudulent website (also called phishing site) where you are supposed to log in. Alternatively, you are guided to a website that installs malware on your device.

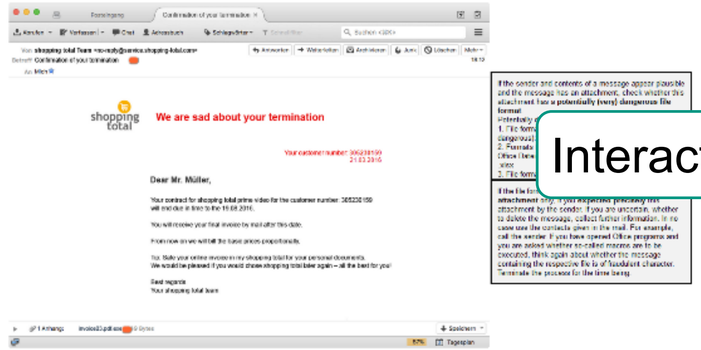
Attachments: messages contain one or several dangerous files (e.g. an attachment of an email). The criminals want to make you open the attachment. By opening or executing the file, malware is installed on your device.

Advertisements: messages may contain ads or other worthless contents (these messages are frequently called spams). The attack is aimed at making you buy something. In reality, the primary damage done is lost working time, because you look at the message, assess it, and delete it.

Text



Video



Interactive Email

Same content

Short-Text

Fraudulent Mails

1. Rule: Check the sender and the contents of every mail for plausibility.

✗ The sender shop@**sye.jp** for an Amazon email
✓ The sender rechnung@**amazon.com** for an Amazon email

2. Rule: Get familiar with where to find the real web address behind a link (e.g. for PCs or laptops in the tooltip or the status bar).

3. Rule: Identify the whois of the web address.

https://nophish.**amazon.com**/login

4. Rule: Check, if the whois matchs with the supposed legit mail.

✓ https://www.**my-parcelservice.com**/
✗ https://www.my-parcelservice.com.**online-shopping.com**/
✗ https://**online-shopping.com**/my-parcelservice.com/
✗ https://www.**129.13.152.9**/secuso.org.secure-login.com/

5. Rule: Check, if the whois is written correctly.

✓ https://www.**farmers-market-total.com**/
✗ https://www.**farmers-rnarket-total.com**/
✗ https://www.**farrners-market-total.com**/
✗ https://www.**farmres-market-total.com**/

6. Rule: 6. If you cannot assess the whois clearly, collect further information, e.g. by searching the address in a search machine.

✓ https://www.**amazon.com**/
✗ https://www.**amazon-shopping.com**/

7. Rule: Check the file format of the attachment.

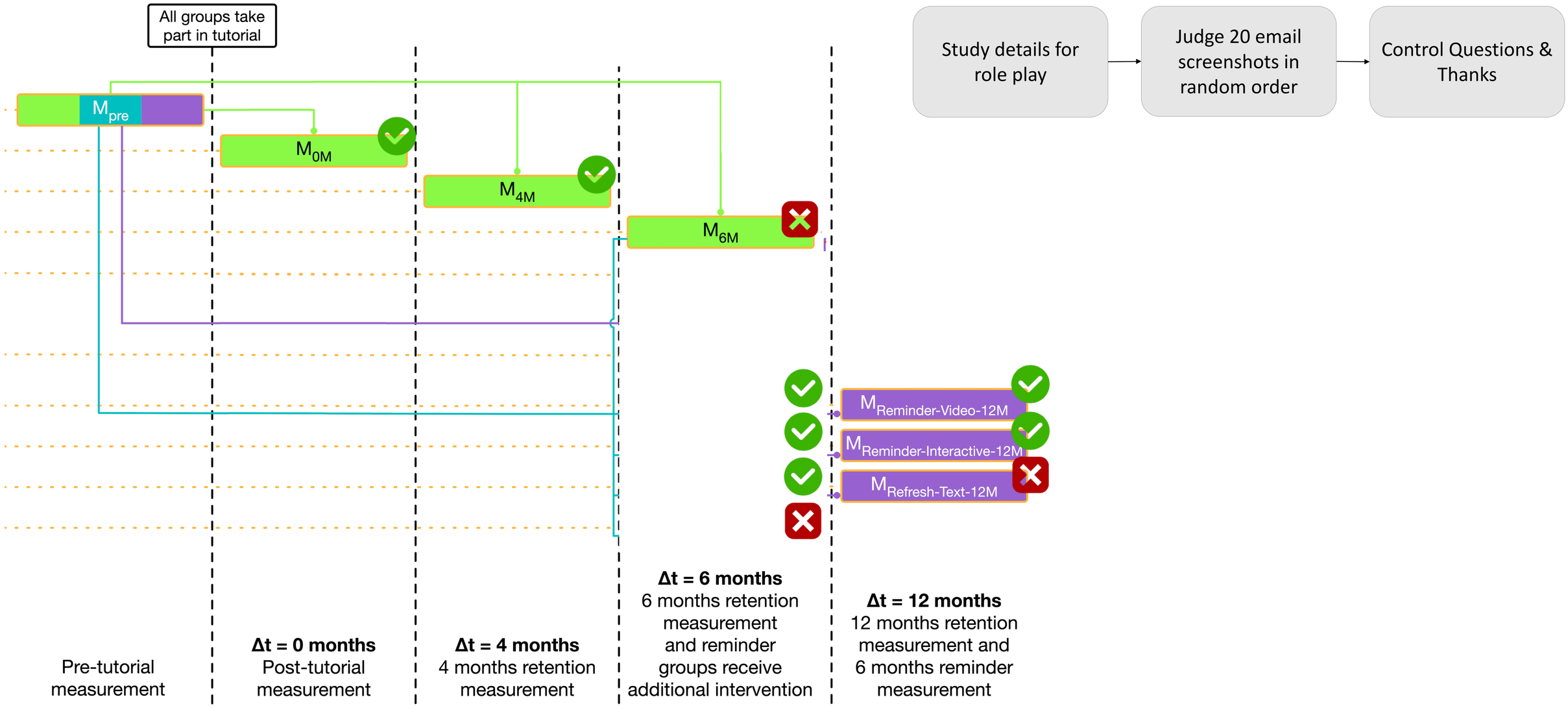
✗ Executable formats, e.g. .exe, .bat, .cmd
✗ Files including macros, e.g. Office files like .doc, .docx, .docm

8. Rule: If you cannot clearly assess the attachment or if you are uncertain about expecting precisely this format by the sender, collect further information, e.g. by contacting the sender. In no case use the contacts given in the mail.

SOUPS 2020, Benjamin Reinheimer
Research Group Security • Usability • Society (SECUSO)

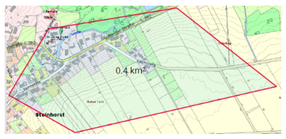
SECUSO SECURITY · USABILITY · SOCIETY aifb KASTEL

Study Design and Results



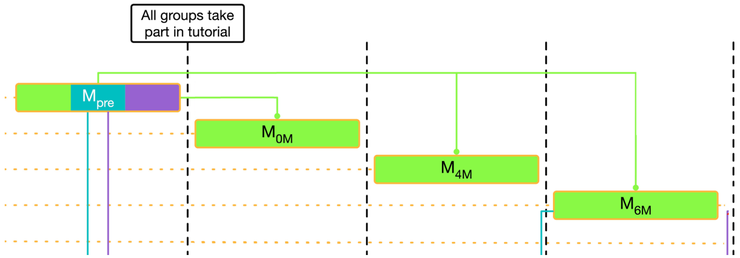
Summary

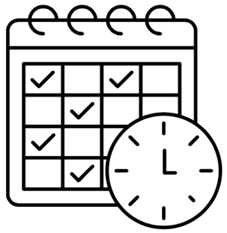
Longitudinal field-study



409 out of 2,200 employees

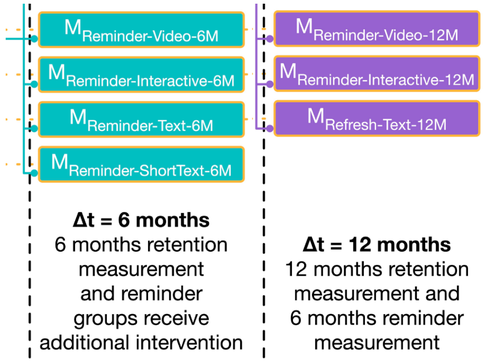
Systematically measure retention





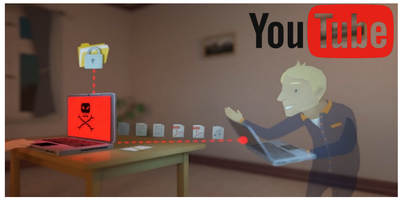
Reminder necessary between 4 and 6 months

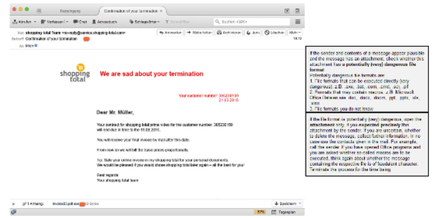
Reminder measures



Δt = 6 months
6 months retention measurement and reminder groups receive additional intervention

Δt = 12 months
12 months retention measurement and 6 months reminder measurement





Video and Interactive Email example most effective

Thanks for listening
and
thanks to my co-authors

For further questions feel free to contact me via
Benjamin.Reinheimer@kit.edu
https://s.kit.edu/soups2020