NoPhish App Evaluation: Lab and Retention Study

Gamze Canova, Melanie Volkamer,
Clemens Bergmann and Benjamin Reinheimer

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

I. Introduction

- Importance for self-reliance
  - ➔ Game-based education app (NoPhish)

- Evaluation
  - Lab Study
  - Retention Study (5 months later)
  - N=19 (m=6, f=13)
  - Age: 20 to 36

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY
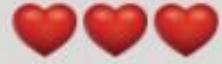
II. Game Design

II. Game Design

- Awareness Part
- Gaming Part: 8 Levels
  - Level 1: structure of a URL
  - Level 2: subdomain trick with very obvious domain name
  - Level 5: subdomain trick with trustworthy/related names
  - Level 7: trick where a character of the domain name is substituted
  - Level 8: trick where the host/brand name appears in the path part of the URL

amazon.phishing.com
amazon.shopping.com
mircosoft.com
auction.org/www.ebay.com

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

III. Lab Study

(1) Informed Consent

(2) Website-Survey Before

(3) Play NoPhish

(4) Website-Survey After
(5) General-Survey After

(6) Certificates and Debriefing

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

III. Lab Study

Hypothesis 1:
  After playing NoPhish, the participants give significantly more correct answers whether or not a website is a phishing website
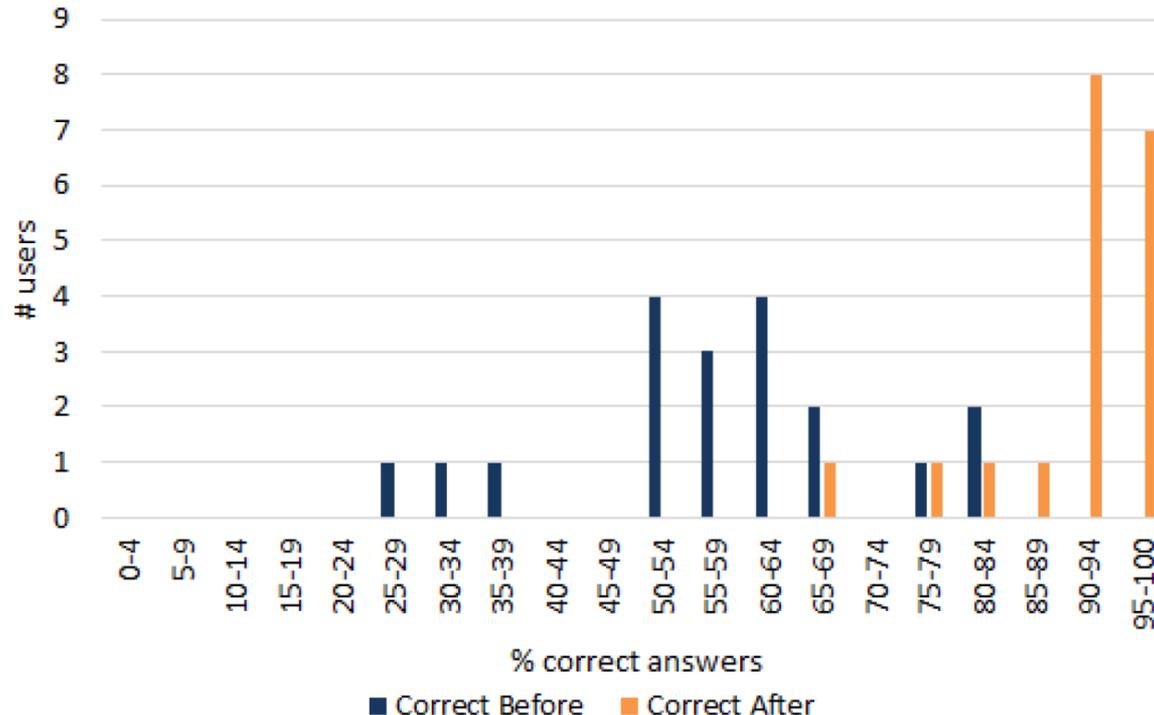
Wilcoxon signed-rank test p-value < 0.001

III. Lab Study

Hypothesis 2:

After playing NoPhish, the participants primarily base their decision whether or not a website is a phishing website significantly more often on the URL

Wilcoxon signed-rank test p-value < 0.001
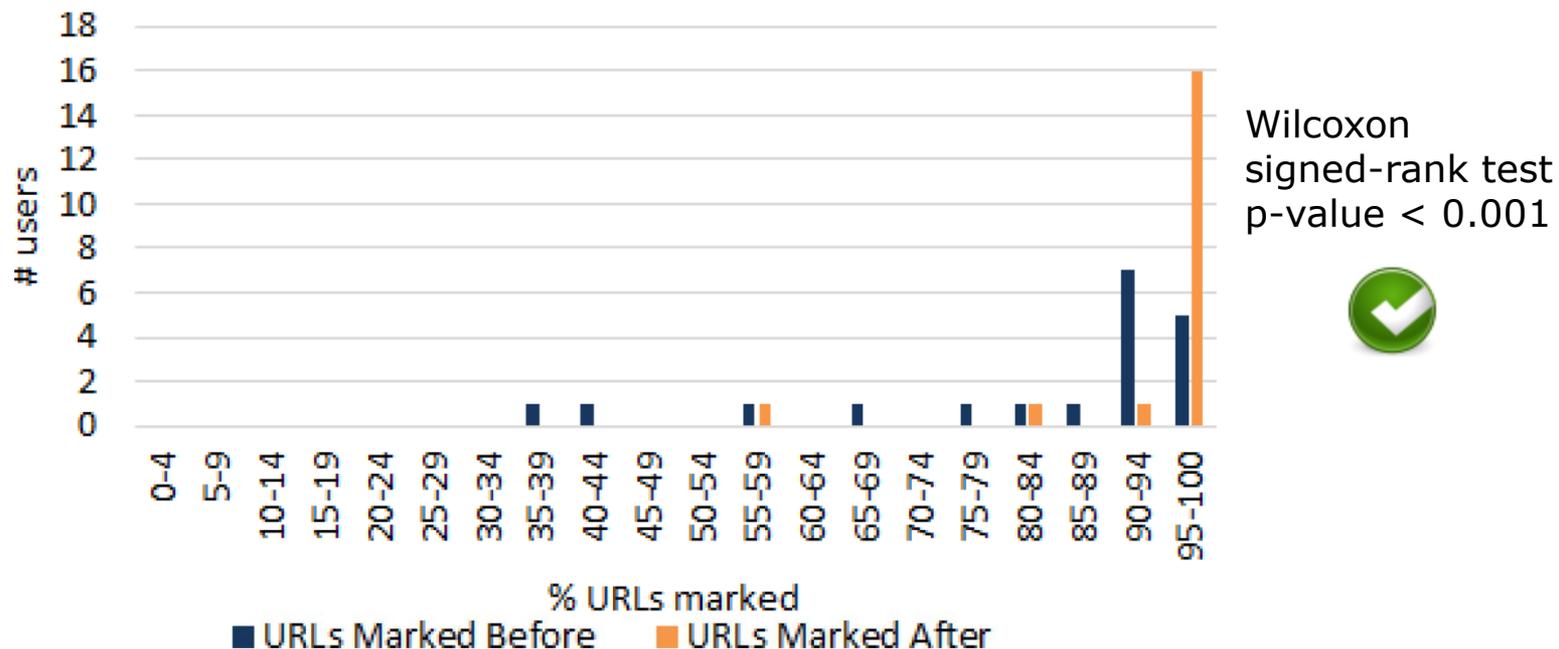
III. Lab Study

Hypothesis 3:

After playing NoPhish, the participants primarily base their decision whether or not a website is a phishing website significantly more often on the domain of a URL
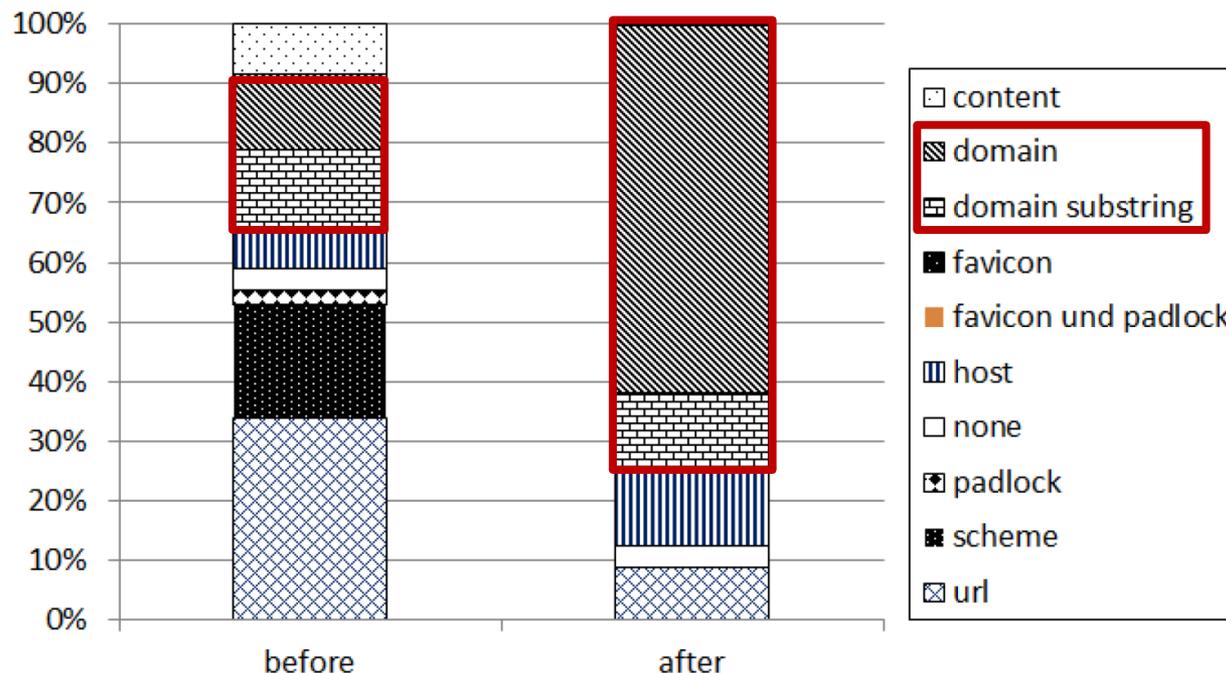
Wilcoxon signed-rank test p-value < 0.001

III. Lab Study – Further Findings

- Confidence - 5 Likert Scale

Before	After
21% with Median of 5 (very certain)	79% with a Median of 5

- Participant opinions – 5 Likert Scale

NoPhish helped me identify phising websites in the future	The text was easy to understand
Median of 5	Median of 5

IV. Retention Study

(1) Phishing Survey

- The 24 examples from the lab study
- 10 new examples (5 phishing & 5 legitimate)
- Confidence about their answers

(2) General Questions

- „Did you receive a phishing email in the last few months?"
- „Do you think NoPhish helped you identify phishing attacks?"

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

IV. Retention Study

Hypothesis 5 – Lab Study Before vs. Retention

In the retention study the participants give significantly more correct answers when deciding whether a website is a phishing website or not than before playing NoPhish.
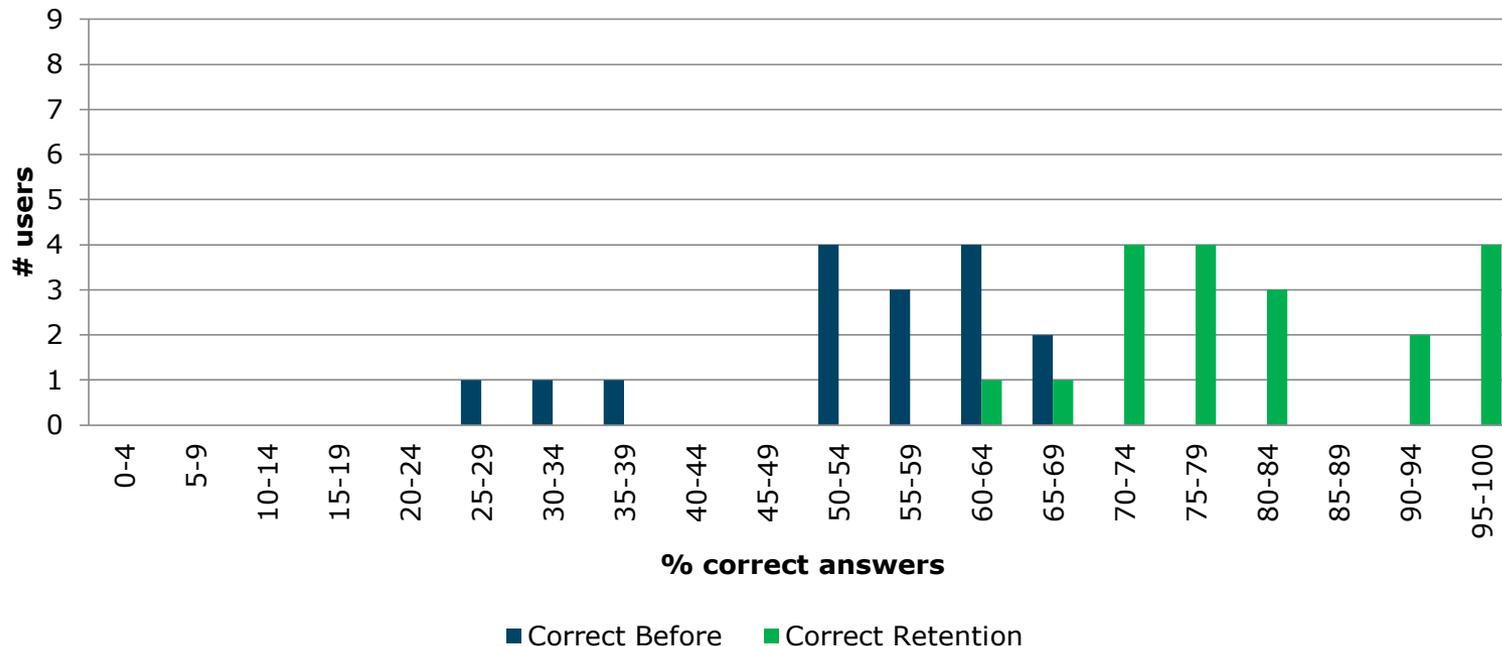
Wilcoxon signed-rank test p-value < 0.001

IV. Retention Study

Hypothesis 6 – Lab Study After vs. Retention

In the retention study the participants do not give significantly fewer correct answers when deciding whether a website is a phishing website or not than directly after playing NoPhish.

Wilcoxon signed-rank test p-value of 0.005

Legend: ■ Correct After   ■ Correct Retention
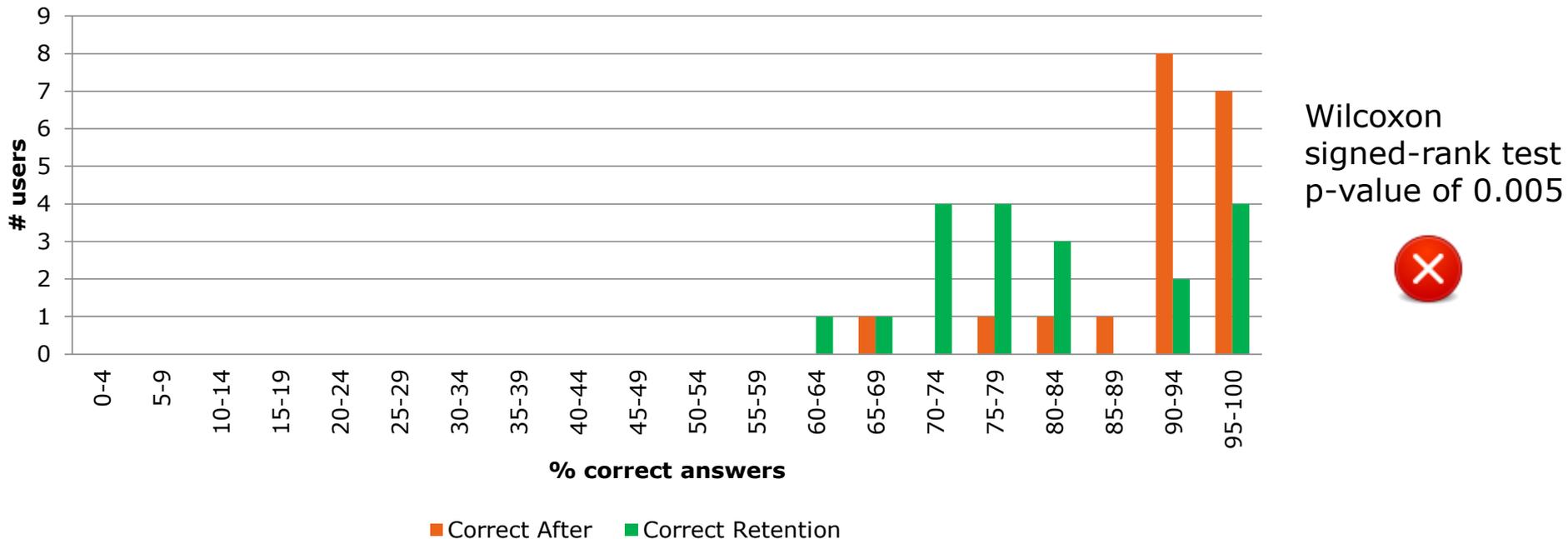
IV. Retention Study

Further Findings

(1) 58% participants detected a phishing attack

(2) 90% =>App (very) important for phishing attack detection

V. Discussion

a. Hypothesis

- (H6) Website-survey after vs. retention

Average After	Average Retention
90,70%	81,89%

- Regression towards the mean

- Exponential nature of forgetting
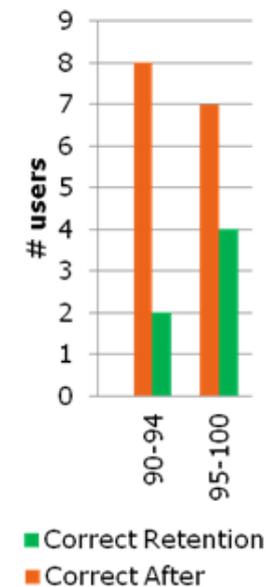
V. Discussion

b. Individual URLs/Levels

1) Subdomain

amazon.shopping.com

Before	After	Retention
✗	✓	!

V. Discussion

b. Individual URLs/Levels

2) Letter swapping trick   mircosoft.com

Before	After	Retention
❌	❌	❌

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

V. Discussion

b. Individual URLs/Levels

3) Legitimate URLs

Before	After	Retention
⊖ Overcaution	✔ Certainty	⚠ Overcaution

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

VI. Conclusion

- Game-based education app
- Phishing detection training
- 3 different points in time

- Significant better performance
- Subdomains Repetition
- More focus on letter swapping
- Comparative Studies
- Perceived app as usefull

References

"Gnome-document-open-recent" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-document-open-recent.svg#mediaviewer/File:Gnome-document-open-recent.svg

"Gnome-document-new" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-document-new.svg#mediaviewer/File:Gnome-document-new.svg

"Gnome-security-medium" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-security-medium.svg#mediaviewer/File:Gnome-security-medium.svg

"Gnome-logviewer" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-logviewer.svg#mediaviewer/File:Gnome-logviewer.svg

"Gnome-application-exit" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-application-exit.svg#mediaviewer/File:Gnome-application-exit.svg

"Gnome-process-stop" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-process-stop.svg#mediaviewer/File:Gnome-process-stop.svg

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

References

"Gnome-accessories-text-editor" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-accessories-text-editor.svg#mediaviewer/File:Gnome-accessories-text-editor.svg

"Gnome-input-gaming" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-input-gaming.svg#mediaviewer/File:Gnome-input-gaming.svg

"Gnome-emblem-documents" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-emblem-documents.svg#mediaviewer/File:Gnome-emblem-documents.svg

"Gnome-dialog-question" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-dialog-question.svg#mediaviewer/File:Gnome-dialog-question.svg

"Gnome-face-cool" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-face-cool.svg#mediaviewer/File:Gnome-face-cool.svg

"Gnome-emblem-default" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-emblem-default.svg#mediaviewer/File:Gnome-emblem-default.svg

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

References

"Gnome-emblem-important" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-emblem-important.svg#mediaviewer/File:Gnome-emblem-important.svg

"Gnome-process-stop" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-process-stop.svg#mediaviewer/File:Gnome-process-stop.svg

"Gnome-application-certificate" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-application-certificate.svg#mediaviewer/File:Gnome-application-certificate.svg

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY