Full Reference:
Nguyen, C., Jensen, M., & Day, E. (2023). Learning not to take the bait: A longitudinal examination of digital training methods and overlearning on phishing susceptibility. European Journal of Information Systems, 32(2), 238–262. Scopus.
https://doi.org/10.1080/0960085X.2021.1931494

Main Points:
Based on the previous study that supports digital training as a way to reduce phishing susceptibility, this study examines the effectiveness and retention of two different digital training methods for phishing awareness over a longer period, and whether overlearning can improve these outcomes. This study provides training sessions of rule-based training, mindfulness training, and control group training for participant students. All the training groups included some participants who received the overlearning procedure. Then the evaluation is conducted through email identification tests and mock phishing messages delivered to their inboxes over both the short term and long term. Results show that compared to rule-based training, mindfulness training resulted in greater retention in terms of better email discrimination and less susceptibility to phishing attacks but similar levels of caution towards phishing. However, overlearning provided limited support for phishing skill retention.

Part Difficult to Understand:
The hypothesis part is difficult to understand at the beginning because the study involves three groups with different time periods for comparison, and an additional factor of whether overlearning is implemented, resulting in seven hypotheses. However, the article provides a clear summary of the hypotheses and a structured table of results, making the complex and numerous hypotheses easier to understand.

Issues to be Discussed Further:
This article selected only undergraduate students for analyzing phishing results in order to remain consistent with previous studies. However, results might differ for employees within companies. Additionally, different age groups, such as teenagers, middle-aged individuals, or the elderly, might have varying susceptibilities to scams. Many further studies could be considered or discussed.

Why Did I Choose This Article:
I have a finance background and the finance industry often needs to handle sensitive data like bank accounts or transaction details. In this case, phishing targeting the high-valuing finance sector is quite common. I have met numerous phishing scams via phone and email, such as shopping discounts, loans, and cryptocurrencies. This triggered my desire to find a solution for phishing activities. In this AI-driven era where phishing activities become increasingly complex

and even pass through the security filter, I believe that the personal level of anti-phishing is really helpful, and this article provides guidelines and instructions for further actions against phishing.

Relation to My Research Interests:
This article focuses on undergraduate students, aged between 18 and 42. My research interest is mainly within the adult learning area, such as career coaching, employee learning, and IT skills development.

How Did I Identify This Article?
Database: Scopus
⇒ Search within Article Title, Abstract, Keywords: IT AND Learning AND Phishing
⇒ Filter: *Limit to*
Year: 2020-2024,
Language: English,
Country: US,
Subject Area: Decision Sciences; Social Sciences; Economics Econometrics and Finance.
⇒ Sort by most cited
⇒ 30 articles appear
⇒ This article has an interesting title. Compared with other articles for example:
Training Users to Identify Phishing Emails
Phishing Evolves: Analyzing the Enduring Cybercrime

Full Reference:

Nguyen, C., Jensen, M., & Day, E. (2023). Learning not to take the bait: A longitudinal examination of digital training methods and overlearning on phishing susceptibility. European Journal of Information Systems, 32(2), 238–262. Scopus. https://doi.org/10.1080/0960085X.2021.1931494

Main Points:

Based on the previous study that supports digital training as a way to reduce phishing susceptibility, this study examines the effectiveness and retention of two different digital training methods for phishing awareness over a longer period, and whether overlearning can improve these outcomes. This study provides training sessions of rule-based training, mindfulness training, and control group training for participant students. All the training groups included some participants who received the overlearning procedure. Then the evaluation is conducted through email identification tests and mock phishing messages delivered to their inboxes over both the

short term and long term. Results show that compared to rule-based training, mindfulness training resulted in greater retention in terms of better email discrimination and less susceptibility to phishing attacks but similar levels of caution towards phishing. However, overlearning provided limited support for phishing skill retention.

Part Difficult to Understand:

The hypothesis part is difficult to understand at the beginning because the study involves three groups with different time periods for comparison, and an additional factor of whether overlearning is implemented, resulting in seven hypotheses. However, the article provides a clear summary of the hypotheses and a structured table of results, making the complex and numerous hypotheses easier to understand.

Issues to be Discussed Further:

This article selected only undergraduate students for analyzing phishing results in order to remain consistent with previous studies. However, results might differ for employees within companies. Additionally, different age groups, such as teenagers, middle-aged individuals, or the elderly, might have varying susceptibilities to scams. Many further studies could be considered or discussed.

Why Did I Choose This Article:

I have a finance background and the finance industry often needs to handle sensitive data like bank accounts or transaction details. In this case, phishing targeting the high-valuing finance sector is quite common. I have met numerous phishing scams via phone and email, such as shopping discounts, loans, and cryptocurrencies. This triggered my desire to find a solution for phishing activities. In this AI-driven era where phishing activities become increasingly complex and even pass through the security filter, I believe that the personal level of anti-phishing is really helpful, and this article provides guidelines and instructions for further actions against phishing.

Relation to My Research Interests:

This article focuses on undergraduate students, aged between 18 and 42. My research interest is mainly within the adult learning area, such as career coaching, employee learning, and IT skills development.

How Did I Identify This Article?

Database: Scopus

⇒ Search within Article Title, Abstract, Keywords: IT AND Learning AND Phishing

⇒ Filter: *Limit to*

- Year: 2020-2024,
- Language: English,
- Country: US,
- Subject Area: Decision Sciences; Social Sciences; Economics Econometrics and Finance.

⇒ Sort by most cited

⇒ 30 articles appear

⇒ This article has an interesting title. Compared with other articles for example:

- *Training Users to Identify Phishing Emails*
- *Phishing Evolves: Analyzing the Enduring Cybercrime*