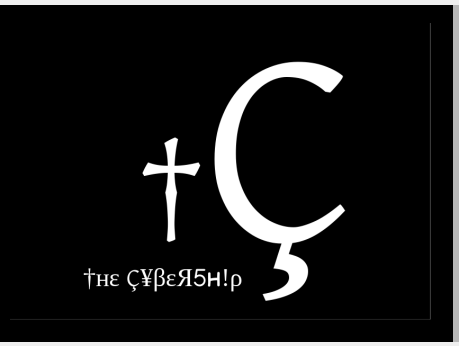


Cybersecurity Course Material

Powered by Hack Sparrow
and Elisabeth Exploidian

Awareness

"You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable."

Daryl White, DOI CIO



Table of Contents

Table of Contents **2**
Introduction **4**
How effective is security awareness training? **5**
Asking the IT staff… 5
Following the results 5
What makes security awareness successful? **7**
Keep it regular 7
Keep it engaging 7
Cover one essential topic, but cover different topics in different campaigns. 7
Measure the impact of training 8
The SANS Security Awareness Maturity Model **9**
Stage 1 10
Stage 2 10
Stage 3 10
Stage 4 10
Stage 5 10
International and national awareness **11**
European Cybersecurity Month 11
Centre for Cyber Security Belgium 12
Safeonweb 12
CCB campaigns 13
Campaigns Materials 13
Campaign 2024 13
Campaign 2023 13
Campaign 2022 14
Campaign 2021 14
Campaign 2020 14
Internal awareness campaigns **15**
Campaign 2025 15
Campaign 2024 15
Campaign 2023 15
Campaign 2022 16
The Topic 16
Goals 16
Result 16
Campaign 2021 17
Campaign 2020 18
What Makes a Good Awareness Campaign? **19**
Clear and Simple Message 19
Relevance and Recognition 19

Accessibility and Availability 19
Interactive and Engaging 19
Repetition and Continuity 19
Five takeaways for a successful campaign provided by the CCB 20
Campaign 2026 20
Assignments 21
References 23



Introduction

🧠Remember our course on Social Engineering.🧠

We've seen that security incidents often stem from human error, making security awareness a crucial aspect of any organization's defense strategy. A well-informed individual can recognize threats, avoid common pitfalls, and contribute to a safer online environment.

This document explores the importance of security awareness and the key elements of effective awareness campaigns. We will highlight best practices to engage individuals and organizations in fostering a security-conscious culture. Additionally, we will provide insights into the free awareness campaigns offered by Safeonweb.

By implementing the right awareness initiatives, we can collectively reduce risks and create a more secure digital world.

How effective is security awareness training?

Asking the IT staff...

If you ask IT staff about the success of an awareness campaign, you'll get a variety of answers. Here are a few examples...

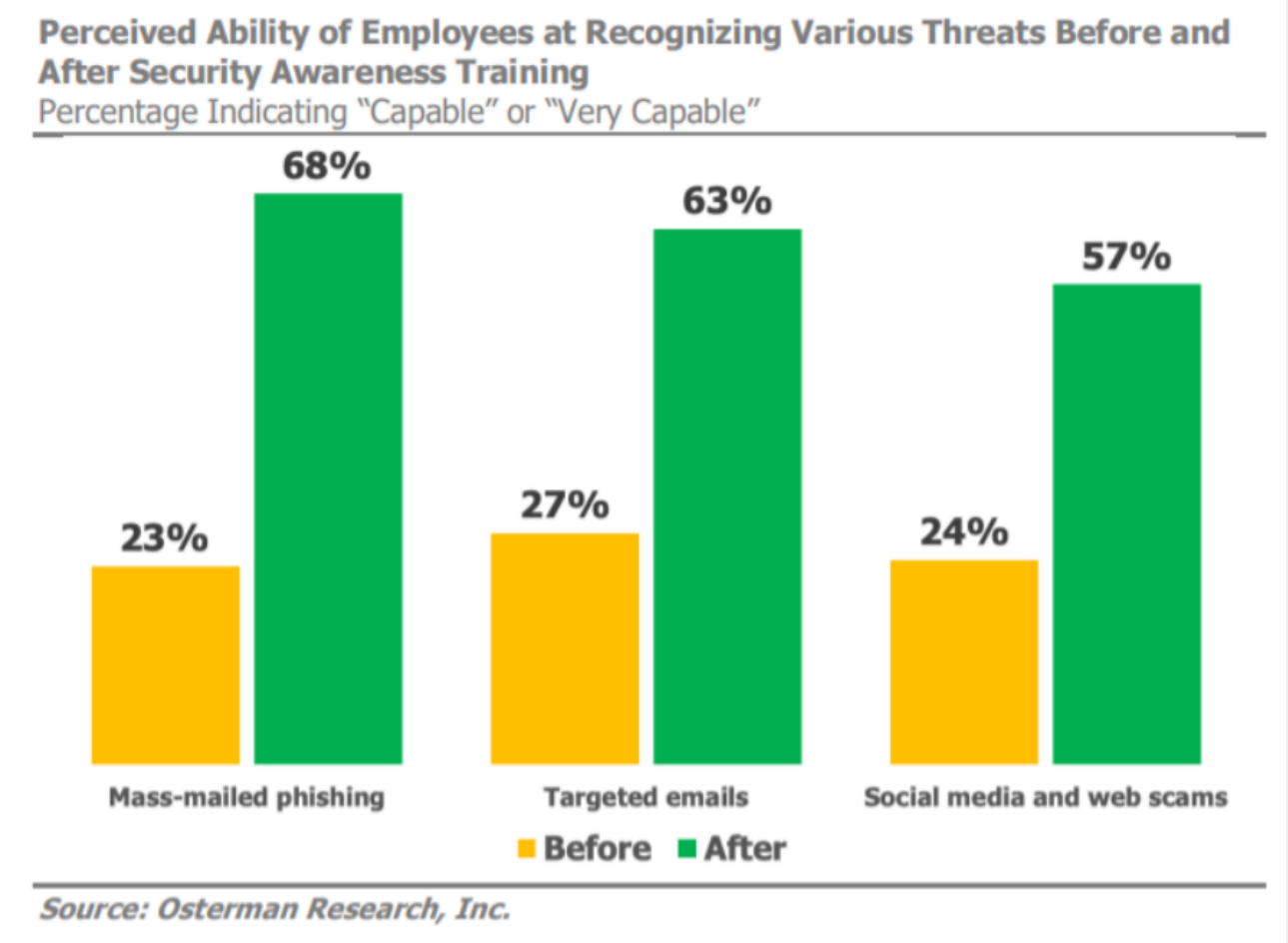
- Nobody called the helpdesk asking how to send their bank details to a Nigerian prince – so, progress!" 💰🚫
- We sent a fake phishing email, and instead of clicking, people reported it! Miracles do happen!" 🎉
- Karen from accounting didn't write her password on a sticky note this month. We're basically cybersecurity legends now." 🏆
- The number of people using 'Password123' went down by 50%. The other 50%... well, we're still working on them." 😅
- Bob from sales actually questioned an email from 'IT Support' asking for his credentials. Our work here is done! 🎓
- The CEO didn't fall for a phishing scam this quarter. That's a first! 🤯
- No one tried to plug in the random USB we 'accidentally' left lying around. We might just cry happy tears. 😂

Following the results

Following a study done by Osterman Research[1], 80% of organisations said that security awareness training had reduced their staffs' susceptibility to phishing attacks. That reduction doesn't happen overnight, but it can happen fast with regular training being shown to reduce risk from 60% to 10% within the first 12 months.

[1] https://blog.usecure.io/does-security-awareness-training-work

The graph below gives a visual insight into one study that measured how staff were able to recognise threats before and after training.



Following IMS[2] the impact of security awareness training can be seen on different levels.

- 70% drop in phishing-related incidents
- It can reduce the risk of data breaches by 30%
- Companies save substantially on costs related to recovery, legal fees, and potential regulatory fines caused by data breaches
- 50% reduction in incident response time by enabling employees to promptly report and mitigate threats before they escalate
- 30% improvement in password security
- 40% improvement in how employees engage with security initiatives
- 25% reduction in insider threats
- 60% rise in overall employee security awareness

---

2 https://www.imssolutionsgroup.com/resources/blog/the-impact-of-security-awareness-training-key-statistics/

What makes security awareness successful?

Keep it regular

According to USENIX[3] employees will start to forget their training after four months. So delivering regular awareness sessions is key for making sure that the information is kept fresh in their minds.

Keep it engaging

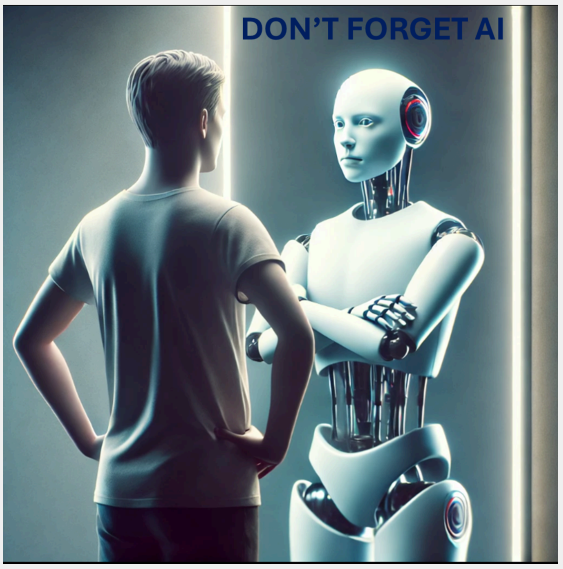
Rather than broadcasting a checklist of points during a PowerPoint presentation, try to deliver something more memorable like a video, an interactive computer-based training/game, a fun flyer/poster, an escape room,..

Cover one essential topic, but cover different topics in different campaigns.

It's easy to think that training staff on how to spot a phishing attack is enough to reduce human risk, but narrowly focusing on a select few topics leaves the door wide open for human error and successful attacks.
Your employees' ongoing training should cover a wide variety of behavioural tips, attack techniques and compliance standards.

Here are 12 security topics you need to know.[4]

- Phishing attacks
- Removable media
- Passwords and Authentication
- Physical security
- Mobile Device Security
- Working Remotely
- Public Wi-Fi
- Cloud Security
- Social Media Use
- Internet and Email Use
- Social Engineering
- Security at Home
- The danger of AI



[3] https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf
[4] https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020

Measure the impact of training

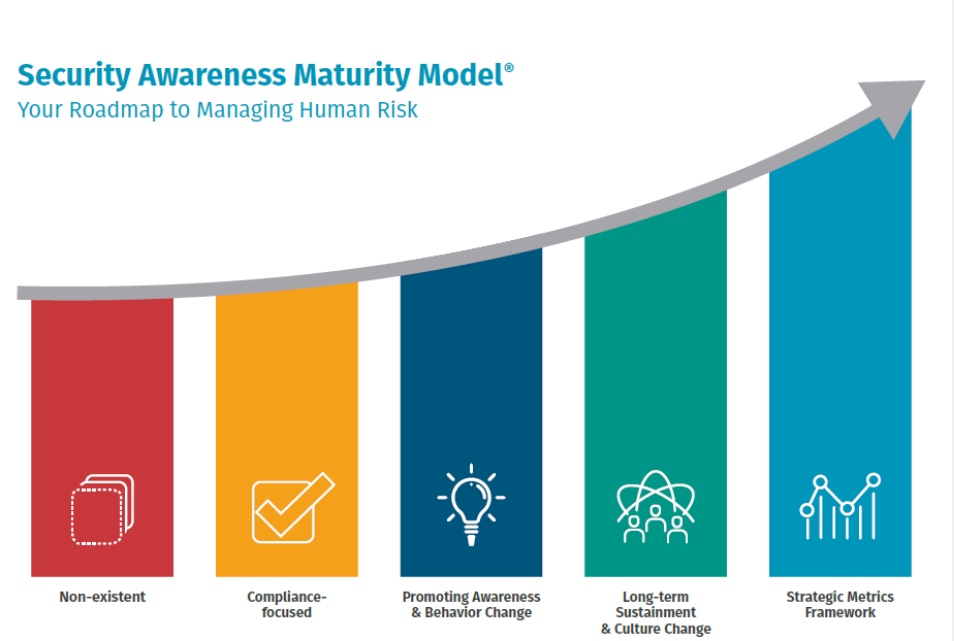
It's important to measure the impact of training so that your business can

- report on whether your approach is working
- have a birds-eye-view of any potential human risk areas

Running a quick quiz at the end of each training session is a good way of understanding what each person has learned.

The SANS Security Awareness Maturity Model[5]

The SANS Security Awareness Maturity Model® is a powerful tool and detailed roadmap for building your security awareness program, no matter what stage your organization is at in your development.
The model helps organizations self evaluate their current place on the cybersecurity evolutionary scale, learn to develop security operations further, and determine how to communicate strategy and results to leadership and sustain their support.



[5] https://www.sans.org/security-awareness-training/resources/maturity-model/

Stage 1

In Stage 1, your security awareness program does not exist. Employees have little knowledge that they could be a target, or what to do if they are, and don’t understand that their actions directly impact the organization’s security. There are no tracking metrics and no thought given to how the organization can evolve its security awareness.

Stage 2

A security program exists, but is designed to meet specific compliance or audit requirements and nothing more. Training is limited to an annual or ad hoc basis.

Stage 3

Your program identifies and focuses on the target groups and training topics that have the most significant impact on keeping the organization safe. The program goes beyond sporadic or annual training in favor of regular and ongoing engagement, with content encouraging behavior change at work and home communicated effectively.

Stage 4

At Stage 4, your program has become an integral part of your organization’s culture. It has the processes, resources, and leadership support necessary to sustain itself indefinitely.
The program is dynamic, continuously evolving, and goes beyond simply changing behaviors – it influences employee beliefs, attitudes, and perceptions about security. Security awareness is no longer just a part of operations but is woven into the fabric of your organizational culture.

Stage 5

Stage 5 is the final evolutionary benchmark in the SANS Security Awareness Maturity Model®. At this stage, your program’s robust metrics framework is fully aligned with the organization’s mission, tracking progress and measuring impact for continuous improvement. Beyond measuring behavior and culture, Stage 5 focuses on how these changes reduce risk and support leadership in achieving strategic priorities. The program can easily demonstrate Returns on Investment. While metrics are important at every stage, Stage 5 emphasizes that a mature program must demonstrate a tangible, measurable impact.

International and national awareness

European Cybersecurity Month

The European Cybersecurity Month (ECSM) is the European Union's annual campaign dedicated to promoting cybersecurity among EU citizens and organisations, and to providing up-to-date online security information through awareness raising and sharing of good practices.

Each year, for the entire month of October, hundreds of activities take place across Europe, including conferences, workshops, training, webinars, presentations and more, to promote digital security and cyber hygiene.

The ECSM campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, and supported by EU Member States and hundreds of partners (governments, universities, think tanks, NGOs, professional associations, private sector business) from Europe, and beyond.

The EU Agency for Cybersecurity coordinates the organisation of the ECSM campaign by acting as a "hub" for all participating Member States and EU Institutions, and by providing expert suggestions, generating synergies and promoting common messaging among EU citizens, businesses and public administration. The Agency also publishes new materials and provides expert advice on different cybersecurity topics for Member States' audiences.

https://cybersecuritymonth.eu/
https://cybersecuritymonth.eu/resources/awareness-tools



Centre for Cyber Security Belgium

The Centre for Cyber Security Belgium (CCB) is the central authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the implementation of the Belgian cybersecurity strategy.

The CCB was created by Royal Decree of 10 October 2014 establishing the Centre for Cyber Security Belgium and is under the authority of the Prime Minister.



The Belgian Centre for Cyber Security is led by its Director Miguel de Bruycker, who is assisted by Deputy Director Phédra Clouner.

Miguel de Bruycke
Phédra Clouner

Safeonweb

Safeonweb is an initiative of the Centre for Cyber Security Belgium (CCB). Safeonweb wants to inform and advise Belgian citizens quickly and correctly about cybersecurity, major current digital threats and online safety.

Safeonweb now also has an app that allows you to stay informed in a quick and easy way. This application alerts you to cyber threats and online scams. The Safeonweb app sends two types of alerts: 'Threats', if an infection on your registered home network has been reported to Safeonweb, and 'News', which is about the general cyber threat in our country.

https://www.safeonweb.be/en/safeonweb-app
https://play.google.com/store/apps/details?id=be.ccb.safeonweb&gl=BE

CCB campaigns

The Centre for Cyber Security Belgium (CCB) and the Cyber Security Coalition launched their National Cyber Security Awareness Campaign each year, during the European Cyber Security Month in October.

Campaigns Materials

https://safeonweb.be/en/campaign-material
https://www.youtube.com/@safeonwebbe

Campaign 2025

Stay alert when investing online.

Online investment fraud cost Belgians almost €15 million in the first half of 2025, according to new figures from the FSMA. False trading and crypto platforms are particularly responsible for the damage: a good €12 million was stolen through these channels, which is three times more than in the same period last year.



Campaign 2024

Two-Factor Authentication (2FA).

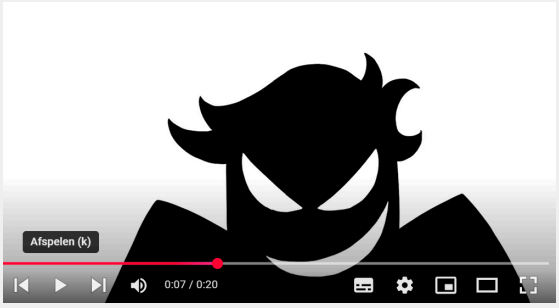
Every day in our country, at least one company falls victim to a cyber attack with serious consequences. What many serious cyber incidents have in common is the absence of two-factor authentication. Up to 80% of incidents could have been avoided if two-factor authentication had been used.



Campaign 2023

Phishing, the devil is in the details!

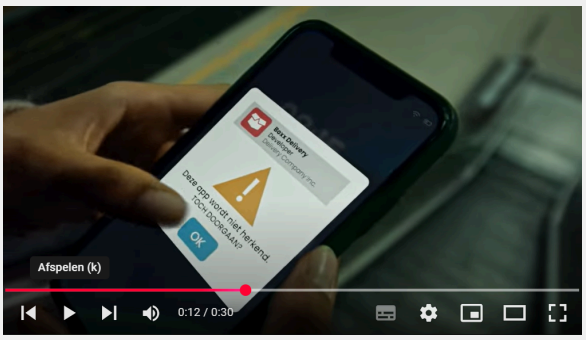
The campaign is yet another reminder of the need to recognise the traps set by cyber criminals. In the case of phishing, this means paying attention to the domain names (URLs) of fake sites. These are identical in appearance to official or trusted sites, except for a few details.



Campaign 2022

OK is not always OK!

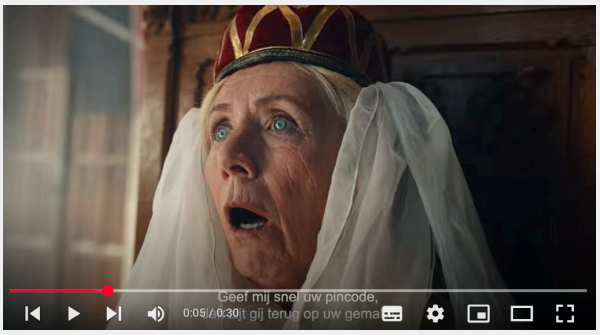
Keeping your smartphone safe is not that difficult. The main way devices get infected is by downloading dodgy apps. Therefore, be careful if you receive an e-mail or a text message asking you to download an app. Chances are you will install a dangerous app or even a virus via an unsafe app shop.



Campaign 2021

Outsmart a phisher.

Be on your guard if you get a suspicious message, and never share personal (response) codes or passwords. In other words: outsmart the phishers.



Campaign 2020

Passwords are a thing of the past. This campaign will fully focus on **two-factor authentication or 2FA**. They want to encourage Internet users to better secure their accounts by means of two-factor authentication.



Internal awareness campaigns

Campaign 2025

The result of this awareness campaign was a short movie, from a group of students, for a group of people close to these students. Think about your family, your youth club, your sports team, or any other community you're a part of.

An example: Team1

Campaign 2024

This campaign was created for a non profit organisation. The main goal was creating different campaigns to make the employees aware of different security topics.

Results of the campaign where

- Impersonating a telenet employee checking physical boundaries
- A phone call created with AI imitating the voice of the head of the IT department with the urgent request to pay an invoice (here or here)
- An escape room covering the risks of keeping passwords and pin codes in unsafe places
- A phishing quiz with different kind messages that looked like those from the organization
- A flyer with a QR code asking to fill in a survey,redirecting those who submitted the survey to a page with key points for secure scanning QR codes
- …

Campaign 2023

This campaign was provided for Thomas More. The campaign was focusing on passwords. The results were a poster provided with a QR code referring to an awareness movie.

Example

Op avontuur naar een wachtwoord van lange duur (poster and movie)

Campaign 2022

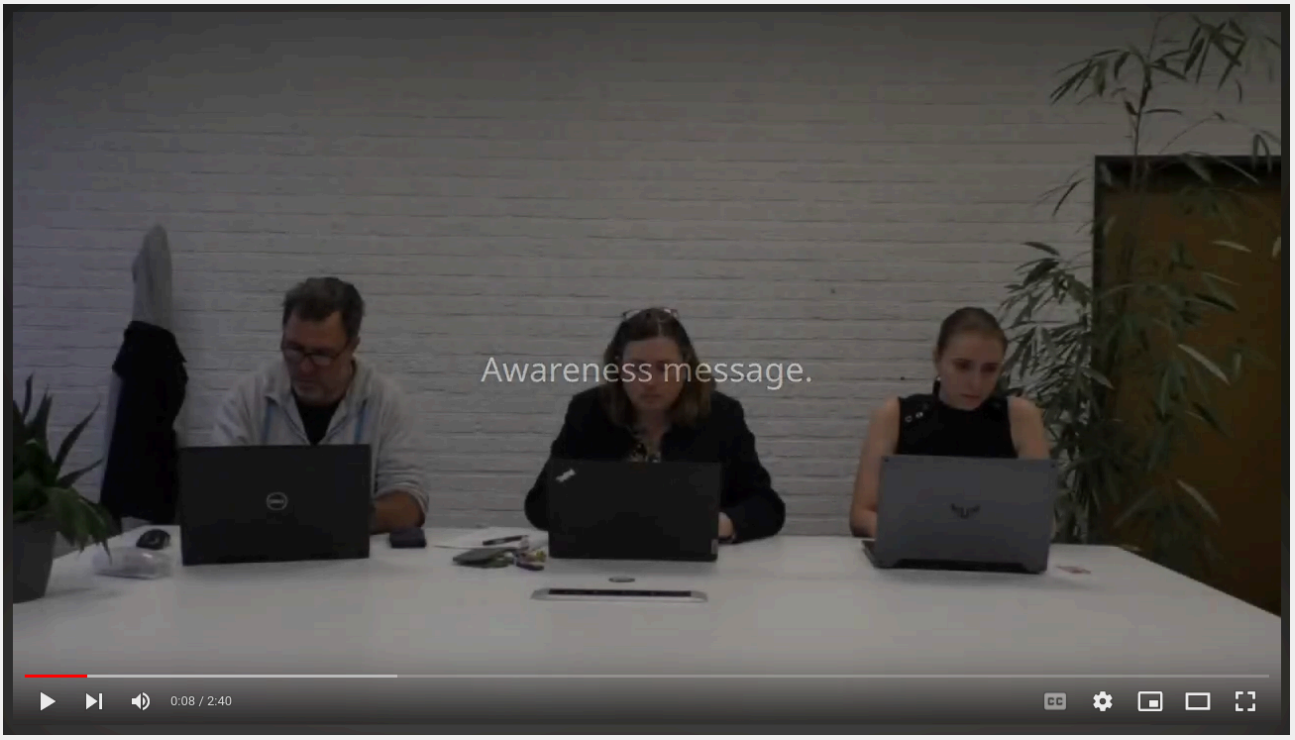
The Topic

https://netstandard.com/why-you-should-always-lock-your-computer/

Goals

- A person knows why he have to lock his workstation
- A person knows how he can lock his workstation

Result



https://youtu.be/BQIm95XUAHM

Campaign 2021

Create your own small awareness campaign on a topic of your choice.

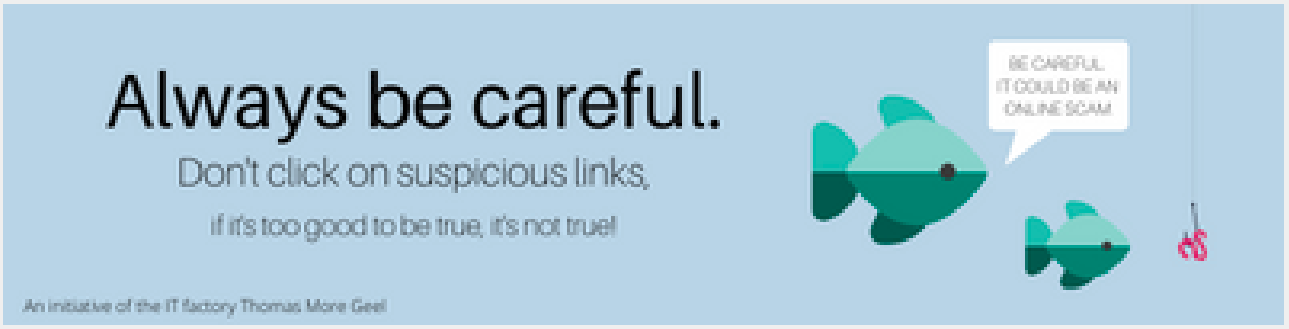
The delivered material should be a banner usable in an email. We'll use this material in a campaign at Thomas More, in the security audit and in our cybersecurity courses for companies.

The banner size should be 300 to 400 pixels wide and 70 to 100 pixels high. The image should also be optimized for a web resolution of 72dpi so it displays correctly.

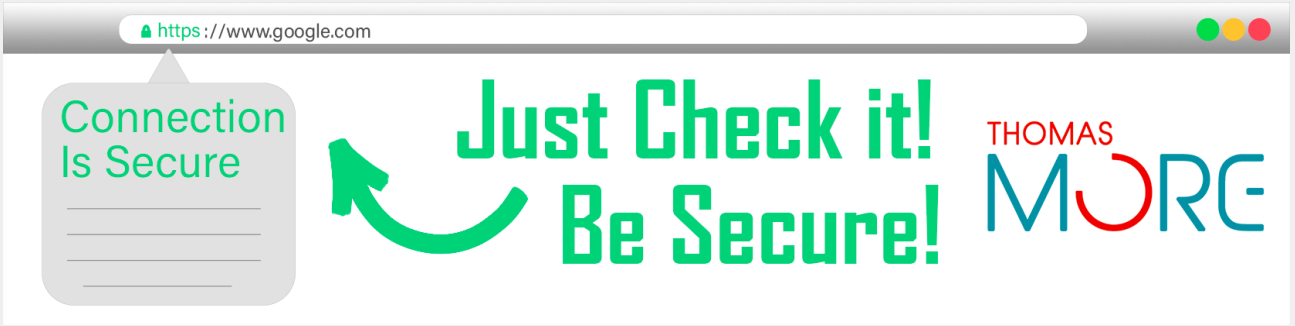
Be creative, make it usable and make it comprehensible, people with no technical knowledge must understand the point you make. No inspiration? https://www.soocial.com/cyber-security-slogans/

There is one mandatory element. It must be made clear that it is "an initiative of the IT factory Thomas More Geel".

The awareness campaign can be on different topics like phishing, vishing, smishing, passwords, backup, spam, lock your device, sexting, …



By Lien Houdenaert - 2021



By Warre Kiekens - 2021

Campaign 2020

Posters about phishing, created for theCybership to put on the awareness wall in the hallway of theCybership.

What Makes a Good Awareness Campaign?

Clear and Simple Message

- Avoid technical jargon and keep the message understandable.
- Use concrete examples and real-life scenarios.

Relevance and Recognition

- The campaign should align with the daily work and experiences of the target audience.
- Use realistic threats and cases that are relevant to the organization.

Accessibility and Availability

- Ensure that employees can easily access the information and training.
- Use different formats (online, in-person, short videos, infographics).

Interactive and Engaging

- Incorporate simulations, videos, games, or quizzes.
- Organize workshops or live demonstrations.

Repetition and Continuity

- A one-time campaign is not enough; regular updates and reinforcement are essential.
- Use multiple communication channels (posters, emails, intranet, presentations).

Measurability and Follow-up

- Conduct tests, such as phishing simulations, to measure effectiveness.
- Analyze results and adjust the campaign as needed.

Support from Management

- Leadership should actively support the campaign and set a good example.

Five takeaways for a successful campaign provided by the CCB

- Set a realistic goal and choose one target audience
- The user is not the weakest link
    - don't put all the blame on the victim
    - don't put all the responsibility on the ‘ordinary’ internet user
- KISS: keep it short and simple
- People are afraid of IT: use a confident touch of humour to keep it light and to attract attention
- Provide a successful experience, the **“Yes, You Can”** feeling!

Campaign 2026

This year we’re going for an individual task. You're going to create an awareness campaign (the result will be a short movie, 45 sec. max) for a group of people close to you. Think about your family, your youth club, your sports team, or any other community you're a part of. Choose a topic that this group can relate to in their everyday lives. Then, develop a scenario around this topic and write a brief script outlining the different steps. Be creative, and make it fun for your audience!

Once you've completed your script, you'll receive feedback, and after that, you can start making your video.

You can use all the AI Tools available, for all steps of the process.

At the end of the movie you include the following banner:

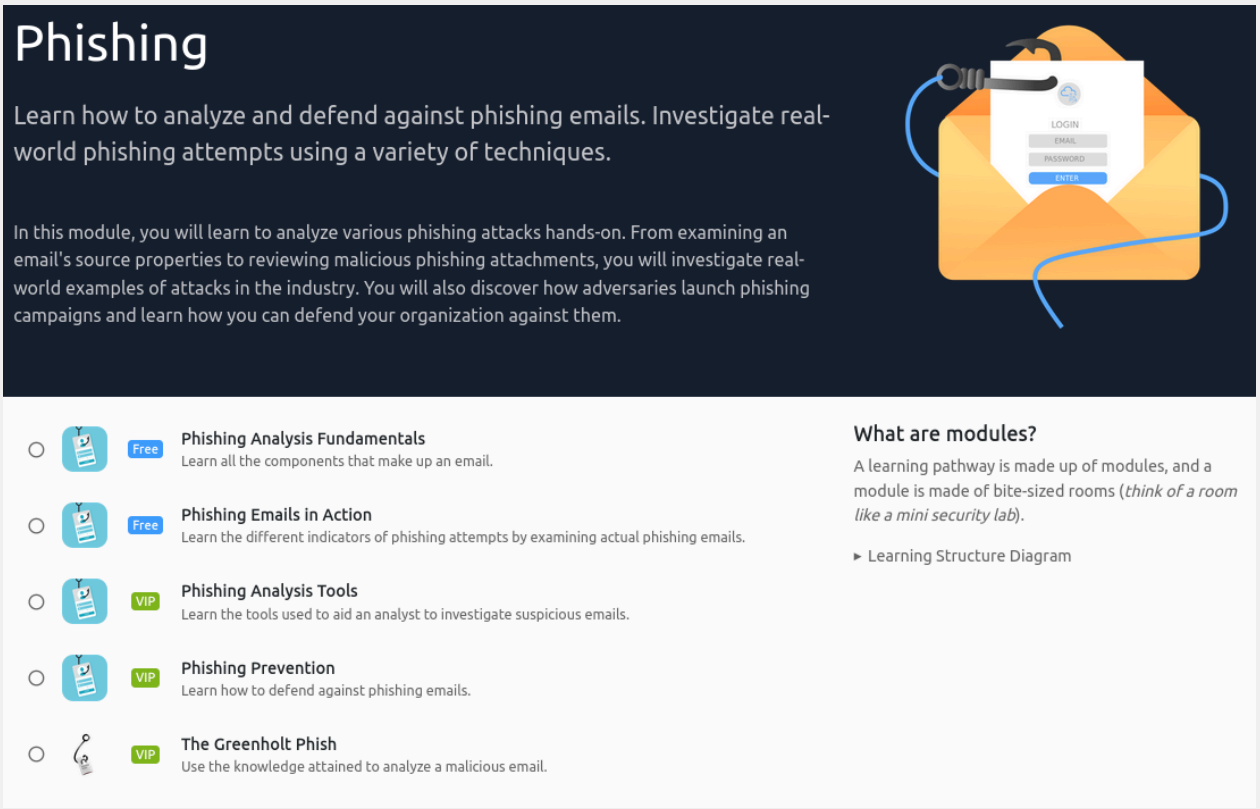


You can download it here.

Assignments

Assignment: THM - Phishing

It’s important as a defender to learn how to analyze and defend against phishing emails. In these rooms, you will learn to analyze various phishing attacks hands-on. From examining an email's source properties to reviewing malicious phishing attachments, you will investigate real-world examples of attacks in the industry. You will also discover how adversaries launch phishing campaigns and learn how you can defend your organization against them.



Mandatory room: https://tryhackme.com/room/phishingemails1tryoe
Mandatory room: https://tryhackme.com/room/phishingemails2rytmuv

Assignment: THM - Security Awareness

Become cyber aware and protect yourself from common security attacks by working through interactive real-world scenarios.

Because as a cyber defender, you are at the heart of your organisation and you play a key role in keeping it safe against cyber attacks. Understand what it takes to be security conscious by walking through the most common attacks seen in the industry, and learn how to mitigate potential threats. Become more security-aware and improve your cyber hygiene in this module.



Mandatory room: https://tryhackme.com/room/securityawarenessintro

References

https://cybersecuritymonth.eu/

https://www.soocial.com/cyber-security-slogans/

Phishing | Met deze tips herken je een goede of slechte url

https://cybersecurity-bites.be