Phishing Simulation Checklist

Here are our recommendations for what you should do before, during, and after every phishing campaign

Before the simulation - Prepare yourself and your organization

*If this is your **first** campaign*

- We recommend you communicate to your organisation that you will be doing phishing training, and that you will have access to the results. You can find the reasoning for this here and a template for communicating this to your organisation.
- Remind your organisation where they can find the appropriate security
  - Don't have a clear process? The training will help you identify areas that need attention.

Before every phishing campaign

- [ ] Tell those who could shut down a real attack that you're doing a test and to let it run its course.
- [ ] Set goals for your organisation. Write down how you think you will perform on the campaign.
- [ ] Plan how you'll react. We recommend you act normal during the simulation. Try to keep a poker face. Your reaction will influence how seriously your organisation views the phishing threat.
  - You might want to give positive reinforcement when employees do the right thing. Thank them for flagging the email and using the right reporting procedure.
- [ ] If you will be out of the office on the day of the campaign, how will you measure the response? Maybe you need to designate a colleague to help you record how things went in the office.
- [ ] Remember to whitelist.
- [ ] Confirm that you got the test email and that the links work as agreed.

On the day of the phishing simulation

What to observe and note down

- Conversation in the office
  - # _____ of posts about the email on internal communication channels (e.g., Teams, Slack, email, casual conversations at the coffee machine, warning by "shouting" it out into the open office).

- Reporting of the email – who is reporting and how?

  # _____ of employees who correctly reported the email (following your procedure).

- What is their reaction? (Do they take it seriously, view it as another "test", ignore it, etc.)

  # _____ of openly ***positive*** attitudes you can observe towards the phishing training.

  # _____ of openly ***negative*** attitudes you can observe towards the phishing training.

- Response time

  _____ Time it took for IT manager or person responsible to be alerted to the phishing attempt.

  _____ Time between email sent and entire organisation made aware.

What to review on the platform (metrics from the simulation)

On the platform you can see the data points from your campaign as they come in.

- Link click rate. (Share of users who received the email and clicked the link)
- Conversation rate (Share of users who received the email and submitted data and/or downloaded something)

After the phishing simulation

- ☐ Share the results. **Here's a template you can use for inspiration.**
  - Share the overall results and phishing signs with the entire organisation on a general level - and don't wait too long.
  - Promptly contact those who fell for the test to share feedback.
- ☐ Analyze these results and identify areas for improvement.

  How did the employees perform? How effective is the existing reporting procedure? Are there patterns? Is it always the new employees? Is it always the same department who falls for the campaign?
- ☐ Acknowledge users who regularly report simulated (and real) phishing emails.
- ☐ Follow up with users who regularly fall for the phishing campaigns.