If you want to succeed with your organization’s security awareness program, here are some of the top “faux-pas” you should be sure to avoid.

1. Sending phishing campaigns only every 90 days. Quarterly phishing tests really just take a baseline, whereas phishing users at least once a month is an effective method to groove in making smart security decisions.

2. Sending the same phishing template instead of randomizing the templates to each user, and running campaigns on predictable times like every Monday afternoon.

3. Singling out users that click on a phishing link and making a public example of them. Do not punish employees that make mistakes early on.

4. Sending only phishing attacks and overlooking stepping users through interactive training.

5. Forcing the program through your users throats, and bypassing getting C-level air cover for the program. You want as much buy-in from the get-go as possible.

6. Forgetting to emphasize that this program will also help your users to keep their family safe online.

7. Starting out with 5-star phishing templates that are too difficult to identify.

8. Not reporting the positive results to the stakeholders with graphics that show improvement over time.

9. Neglecting to inform key stakeholders, department managers and tech support before you send the initial baseline test.

10. Not having a good procedure / process that allows users to report phishing emails that they found in their inbox, and not having a Social Engineering Incident Response program.