How to Run Effective Phishing Assessment and Training Campaigns Employees Don't Hate (the "Eleven Commandments")

[**source**: www.infosecurity-magazine.com/blogs/effective-phishing-assessment/] Tyler Benishti, CEO IronScales]

1. **No shaming!** (Don't *ever* publish campaign results publicly)

2. **Teach, don't blame.** (For those who took the bite, make the landing easy. Use positive messages and focus on the learning)

3. **Make it a game!** (Make it fun and interactive – No death by Power Point) Enlist help to invent Phishing attacks for exercises. Create teams to test each other.

4. **Repeat process every two months** (continuous assessment is the right mindset)

5. **Keep the HELP Desk apprised** (don't make them hate training days; limit the number of emails for them to handle)

6. **DEFINITELY include senior management** (usually the main targets)

7. **Time it right** (short, concise. No month-long campaigns. Try morning hours)

8. **Vary types of phishing attacks** (links, attachments, fake websites requesting user names, passwords. Include a few signs so they no its not real)

9. **Use real-life examples** (Start from the ground up, simple before advanced phishing examples)

10. **Enforce training** (They must do it; make them like it)

11. **Measure progress over time for each phishing scenario** (offer prizes for great performance, show-off your top 100)