Security Awareness Training Best Practices

Here are the key things to know when launching a security awareness training program for your end-users!

Use a Training Cadence that Sticks

Short & consistent beats long & rare.

- Monthly micro-training (5–10 minutes)
- Annual baseline training (compliance + policies)
- Day-one training for new hires

Why it works

Frequent, short training improves retention and keeps security top of mind all year long.

Run Phishing Simulations that Teach

The goal is education – not punishment.

- Depending on the industry, users should receive 1-2 simulations per month
- Increase difficulty gradually
- Avoid manipulative or morale-crushing scenarios.

DO
Send a fake billing statement.

DON'T
Send a fake pay raise.

Train on Relevant Topics

Training should match the user and current threats.

- Tailor content by industry, department, & user roles
- Update content regularly to avoid outdated material

Result

Users engage more with training that's relatable and that actually makes a difference.

Lost in the jargon? Use this cheat sheet:

GOOD

- **Decreased click rate means:** Fewer people are likely to fall for scams
- **Increased report rate means:** More people are actively identifying scams so IT can stop them before they get to other users
- **100% completion rate means:** All of your users are informed which is great for compliance and insurance audits.

BAD

- **Increased click rate means:** More people are likely to fall for scams
- **Decreased report rate means:** Fewer people are actively identifying scams to reduce the spread
  Note: This could be a good sign if less spam is being reported. This means, your users are learning the difference between scams (bad) and spam (annoying).
- **Less than 100% training completion rate means:** Not all users are fully informed which could be a risk to your security and a red flag for insurance audits.
- **Users to watch means:** Users are a risk to your security – this is especially bad if it's users most likely to be targeted

Understand Your Goals & Metrics

Track Metrics that Matter

Measure monthly behavioral change with four key KPIs:

- **Training Completion Rate**
  Are employees participating?
- **Users to Watch**
  Who needs additional training?
- **Phishing Click Rate**
  Are fewer users clicking?
- **Phishing Report Rate**
  Are more users reporting?