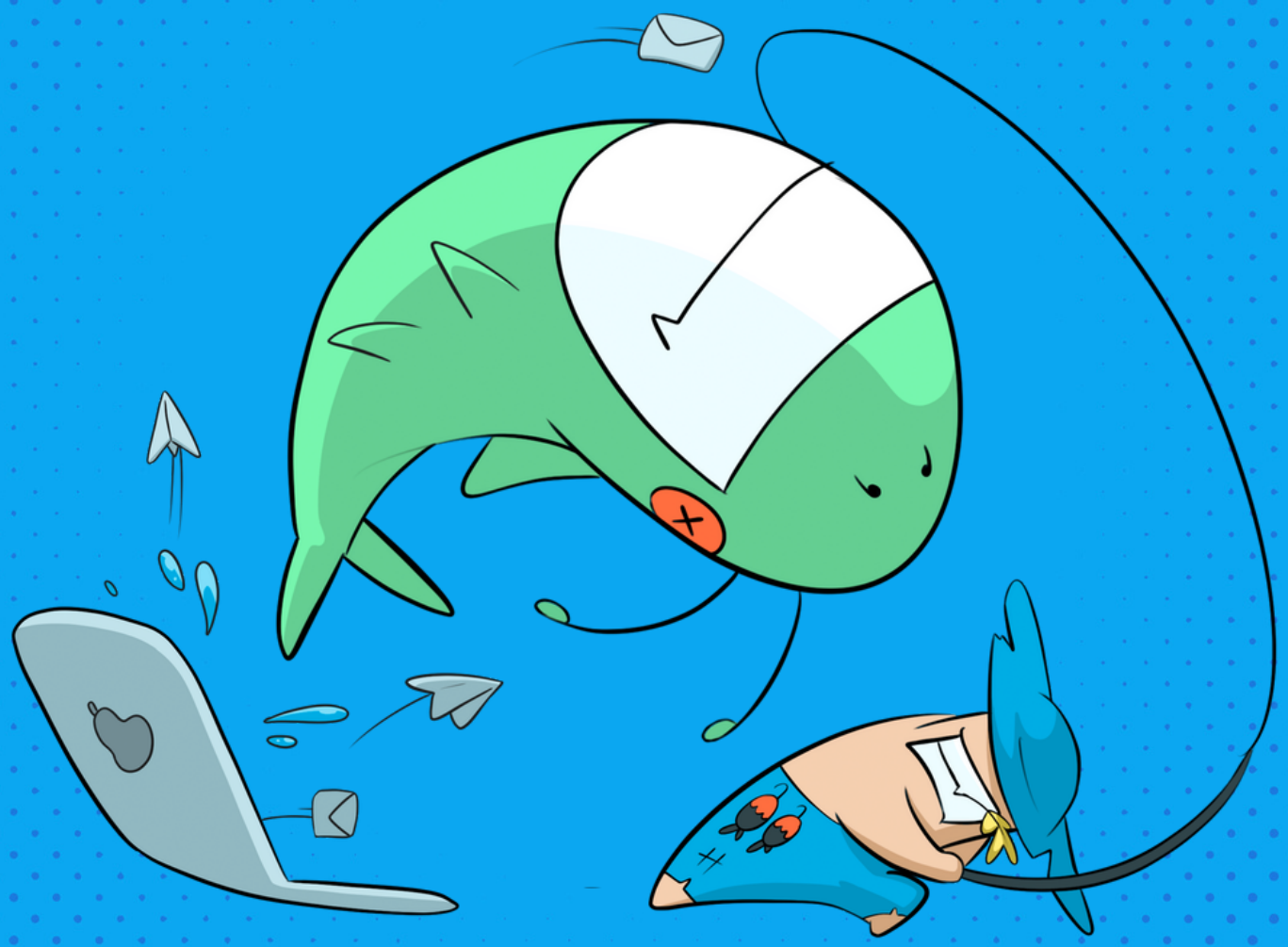
# PHISHING TEMPLATES



The wizer Guide for Effective Campaigns

# USE DIVERSE PHISHING SCENARIOS

**Mix it up with relevant scenarios**, like urgent payment notifications or unexpected Zoom meetings, to illustrate the **impersonation dangers of familiar brands**.

# TRAINING FOCUS

**What we act upon in our inbox every day will always pose a greater risk if it's impersonated.** Providing a safe environment for that 'Oh no, it wasn't real' moment is a valuable learning experience.

# USE EMOTIONAL TRIGGERS WIZELY

**Use non-sensitive topics**, like a missed meeting notification rather than a yearly bonus, **to highlight emotional manipulation**. Avoid offering personal benefits or overly generous or caring messages.

# TRAINING FOCUS

Save real-world examples of how low cyber criminals will go for in-person trainings and not phishing campaigns.

**Scammers are heartless, but phishing sims shouldn’t be!**

# AUTHORITY EXPOSURE

CEO, executive team, managers, or HR make **effective phishing aliases** - it's not easy to say "No" or "Wait" to the higher-ups which is why cybercriminals love to impersonate them.

# TRAINING FOCUS

**Coordinate carefully when impersonating leadership** and be sure you have permission.

Consider this type of phish **for select advanced phishing groups** and not as mass campaigns.

# TIME PRESSURE

**Push the need for speed** in phishing messages.

# TRAINING FOCUS

**Real phishing emails generally give a tighter deadline** than most genuine notifications.

Knowing this can help your team to identify when to **take a step back from messages pushing for a super quick response.**

# CURIOSITY-DRIVEN

Craft messages that **give only part of the details** with the lure of the click to provide the rest of the story - it can be hard to resist!

# TRAINING FOCUS

It’s natural to be curious but **learning to identify when we are is an important** part of developing sensitivity to suspicious situations.

# STAY CURRENT WITH THE TRENDS

**Draw inspiration from current attacks reported** that are most relevant to your organization. Also check with your Security Team on **current threats being caught** to craft highly relevant phishing scenarios.

# TRAINING FOCUS

Use in-person training opportunities to **educate employees on recent threats caught by the organization** - bonus points for celebrating any reported by employees.

# KEEP GOAL IN MIND

**Phishing simulations are best used as a tool to familiarize and build employees' phish-spotting muscles.** Never use it as a 'gotcha' or punitive tool.

**Give proper training before and follow up after** for each phishing simulation run to build trust and create a **positive security culture**.

# Stay wizer

Security Awareness Training & Phishing Simulation

wizer-training.com