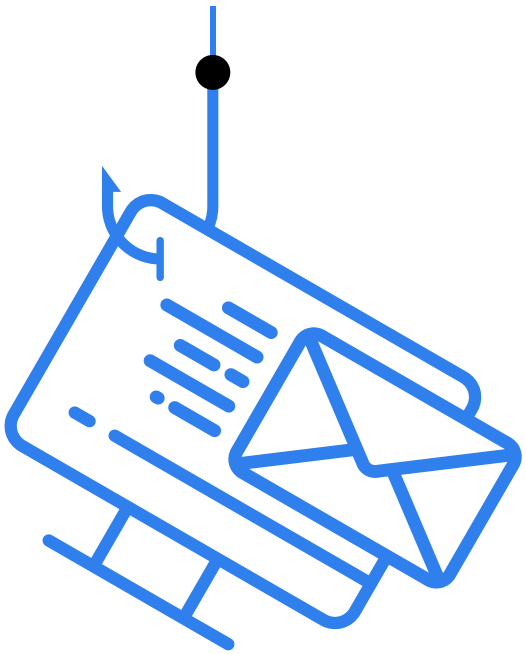
BREAKWATER IT

Simulated Phishing Campaigns

Transform your biggest security risk into your strongest line of defense.

You can invest thousands of dollars in enterprise-grade firewalls, but it only takes one **distracted** employee clicking the wrong link to **compromise** your entire business. Cybercriminals know that hacking humans is significantly easier, cheaper, and faster than hacking software.

At Breakwater IT, we believe your team should be your first line of defense, not your weakest link. We run fully managed, highly **realistic** simulated phishing campaigns to **safely** test your staff. By exposing them to advanced, real-world tactics in a **controlled** environment, we train them to spot and report malicious emails before they face the real thing.



Highly Realistic, Tailored Scenarios We don't use obvious, poorly spelled scam emails from the early 2000s. We simulate sophisticated, modern attacks tailored to your daily operations—such as fake Microsoft 365 login prompts, urgent HR policy updates, or altered vendor invoices.

Safe, "In-the-Moment" Education Our goal is empowerment, not punishment. If an employee falls for a simulated attack and clicks a link, no company data is at risk. Instead, they are instantly routed to a brief, interactive micro-training session that explains exactly which red flags they missed.

Actionable Risk Reporting We provide your leadership team with complete visibility. We deliver plain-English reports showing exactly what percentage of your team is clicking, which types of attacks are most successful, and how your company's overall "security reflex" is improving.

Continuous, Automated Execution Cybersecurity training isn't a once-a-year seminar that employees immediately forget. We manage the entire program silently in the background, sending random, varied simulations throughout the year to keep security top-of-mind without disrupting daily productivity.