

Phishing Prevention Checklist



Use **Phin** to start checking items off your list!

Preventing a breach will always be easier (and cheaper) than responding to one. Here are the tools and systems you should have in place to stay proactive.



SECURITY AWARENESS TRAINING



Implement frequent, engaging, and relevant training for your end-users. A one hour slide show once a year isn't going to cut it. The whole point of training is to change end-user behavior, not put them to sleep. Training should be bite-sized and touch on real world scenarios that your end-users could run into.



PHISHING SIMULATIONS



These should be realistic (but not cruel). When someone clicks on a phishing simulation, they shouldn't be punished with irrelevant training videos. They should receive real-time feedback of what they did wrong, so they know specifically what they need to look out for next time.



REPORT PHISHING BUTTONS



Implement report phishing buttons so users aren't confused about what to do when they come across a phish. It keeps phishing top of mind every time they see the button (there's something so satisfying about reporting an email) and it streamlines reporting, and speeds up investigations.



ANTI-PHISHING BROWSER EXTENSIONS

Deploy solutions to analyze websites for malicious intent and warn users about suspicious sites. These extensions check URLs against databases of known phishing sites, analyze webpage content for suspicious behavior, and warn users before entering personal information. This is a simple added layer of protection.



THREAT HUNTING

Regularly review metrics and reports, block known indicators of compromise (IOCs), and proactively hunt for threats in the system. This will help you identify attacks early and reduce dwell time.



PENETRATION TESTING

Identify vulnerabilities in your email security systems to stay ahead of potential threats. If the good guys can get in, so can the bad guys.

Don't get caught in a phishing attack.

SECURE MY CLIENTS