

User Awareness Training

Key Benefits

- Change users' behavior to reduce risks from phishing and other cyberattacks
- Prioritize and improve incident response
- Fewer helpdesk calls
- Provide consistent training across the globe with multilanguage support
- Track results and progress with real-time reporting
- Reduce successful phishing attacks and malware infections by up to 90%
- Increased reporting of incidents by employees
- Easily view and analyze detailed user-level results, progress, and completion rates across training assignments and modules
- Quickly identify users who need extra training in specific topic areas

ContentCatcher[®]'s built-in Security Awareness Training (formerly Wombat Security) helps you deliver the right training to the right people at the right time, turning your end users into a strong last line of defense to identify cyberattacks and protect your organization.

With more than 90% of cyberattacks starting with an email, wary end users are critical to protecting your people and your data. While technologies that detect and block malicious emails are part of the solution, you can also reduce the likelihood of successful attacks such as phishing or ransomware through effective, broad-based security awareness training.

Protect Your Organization With Phishing Simulations

ThreatSim[®] Phishing Simulations help you understand your organization's susceptibility to a variety of phishing and spear-phishing attacks. With thousands of different phishing templates across 13 categories, you can evaluate users on multiple threat types, including:

- Malicious attachments
- Embedded links
- Requests for personal data

We add multiple templates every week. Our Dynamic Threat Simulation phishing templates are drawn from Proofpoint threat intelligence; others reflect customer requests and seasonal topics. Users who fall for a simulated attack receive practical "just-in-time" teaching. They learn the purpose of the exercise, the dangers of real-world attacks, and how to avoid future traps. You can also help your most vulnerable users by automatically assigning interactive training to anyone who falls for a phishing simulation.

Educate Employees With Engaging, Actionable Training Content

Our growing, continuously updated content library offers video, interactive, and game-based training modules in 35+ languages. Additionally, there is a library of security awareness materials including videos, infographics, newsletters, articles, posters, images and more. All content has consistent, actionable messaging suitable for global organizations. Based on proven Learning Science Principles, our customizable education content covers a broad range of security risks, from phishing attacks to insider threats.

Our training modules are available on demand and are mobile-responsive, so your users can take our training anytime, anywhere, on any connected device, maximizing efficiency and convenience. The modules take an average of just 5 to 15 minutes to complete—minimizing disruption to daily work routines—and the interactive modules conform to the US Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.

We also make it easy to alert your users to the most relevant attacks and lures from Proofpoint threat intelligence with our Attack Spotlight series—brief, timely content that teaches how to spot a current threat and avoid becoming a victim.

Analyze Results With Full-Featured Reporting

Our reporting capabilities provide the granular and high-level visibility you need into your employees' interactions with assessments, simulated attacks, and training assignments. We offer responsive, easy-to-read reporting with a modern UI, providing more than just completion data so that you can evaluate progress, gauge ROI, and benchmark, track, and trend user knowledge. You can use our dashboards to easily filter data, compare assessments, quickly add and remove measures, and more.

You can also download and export data to share business intelligence with other stakeholders, perform more detailed analysis, and evaluate metrics alongside other security events. Our Automated Reporting feature streamlines the export process, allowing you to schedule automatic delivery of reports at regular intervals to yourself and designated stakeholders within your organization.

About Our Continuous Training Methodology

Industry research has shown that once-a-year classroom training is not effective in the battle against cyberattacks. Our unique Continuous Training Methodology is a cyclical approach that teaches users about best practices and how to employ them when facing security threats.

A continuous cycle of assessment, education, reinforcement, and measurement maximizes learning and lengthens retention. Our methodology sits in strong contrast to a "one and done" approach, giving you the flexibility to evolve your program over time, identify areas of susceptibility, and deliver targeted training when and where it's most needed.

Why ContentCatcher®

ContentCatcher was designed from the ground up to deal with the never ending threat of malicious email, and the annoyance of unwanted email.

We believe businesses of all sizes deserve the capability to defend against the evolving email threats we face today. Cloud based email security is the most effective way to increase security and reduce risk in your organization from the most exploited communications channel. In fact, over 35% of organizations who choose Office365 are augmenting that email security with a 3rd party like ContentCatcher.

More info is available at www.contentcatcher.com