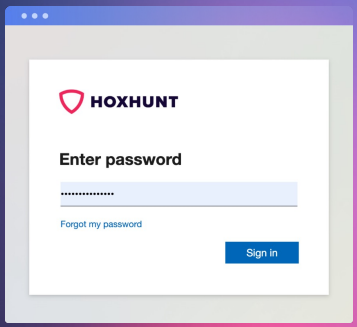
HOXHUNT

Train End-Users to Report Credential Harvesting Attacks

Empower your end-users to detect and report credential harvesting attacks with our advanced phishing training simulations.



One in three data breaches are caused by credential theft. Equip your employees with the skills to manage their credentials securely and quantify your risk levels.

Integrate simulations of well-known login pages into your training, providing instant feedback to end-users as they enter their credentials to improve their skills.

Monitor your performance and track your performance by tracking the number of end-users entering their credentials.

Key benefits

- **Train on safe credential management.** Build up end-users' ability to detect and report credential harvesting attacks.
- **Simulate trusted login experiences.** Mimic sites and login pages that are well-known and trusted by your end-users.
- **Report the amount of entered credentials.** Monitor and report the number of end-users starting to enter credentials.
- **Ensure safe and secure training practices.** Hoxhunt allows you to train your end-users securely, without storing any entered data.

Why Hoxhunt?

Go beyond security awareness. Create lasting behavior change to increase the number of reported real threats.

We offer a complete platform for mitigating human cyber-risk and driving behavior change. Use our solution to create a positive, encouraging, knowledgeable security culture.

Top 50 EMEA Companies 2024 · Best Results Enterprise Winter 2024 · Leader EMEA Winter 2024 · Leader Americas Winter 2024 · Gartner Peer Insights Customers' Choice 2023

★★★★★ TOP PERFORMER AT G2.COM

Measure and enhance your resilience levels

Use the simulated credential harvesting attacks in your phishing training program. Deliver the training to your end-users through adaptive training or scheduled campaigns.

Adaptive training

Use credential harvesting simulations in our AI-powered training program to reduce your human cyber-risk.

- Personalize the phishing training to your end-user's unique skills and role using AI.
- Automate training difficulty, user selection, content, and frequency based on users' performance and your preferences.
- Visualize your onboarding and training activity rates, and the reporting times.
- Track how your end-users improve in reporting, missing, and clicking on the simulated phishing attacks.

Scheduled campaigns

Measure your organization's risk levels by delivering scheduled simulated credential harvesting attacks.

- Select the credential harvesting simulation template that you want to use.
- Select the target group of high-risk end-users that you want to train.
- Send the credential harvesting simulation according to your program's needs.
- Measure your results and report your findings.

Explore how credential harvesting simulations work

Reporing the simulation
The end-user reports the simulation using the Hoxhunt reporting plugin.

Missing the simulation
The end-user does not click on links or enter the credential harvesting landing page.

Failing the simulation
The end-user clicks the email link or starts entering their credentials on the page.

When an end-user leaves the page, we offer the opportunity to earn an additional star.