SECURE MENTEM

WHITEPAPER

A real approach to implementing machine learning to security awareness

Ira Winkler's analysis of Hoxhunt

Why Hoxhunt is Unique:

A real approach to implementing machine learning to security awareness An independent analysis of their phishing engine

By Ira Winkler - https://www.linkedin.com/in/irawinkler/
President, Secure Mentem

SECURE MENTEM

There are so many buzzwords and trends in the security awareness industry that it is hard to determine what is useful and what is a gimmick. Every vendor out there has some sort of promise that they have some special characteristic about their product that makes it a revolutionary improvement to your security awareness posture that no other product can. After reviewing the Hoxhunt solution, it is safe to say that they actually do provide something unique that can really move the needle with your organization's security awareness posture.

Machine learning and artificial intelligence are typically buzzwords and technologies that vendors tout as making a product unique. The reality is that machine learning and AI can be useful, however they are just underlying technologies. It is how you apply the technologies that makes a difference. Hoxhunt uses machine learning in a way that provides a very unique and valuable method for improving security awareness in practice.

Specifically, Hoxhunt uses machine learning in a way to create an individual learning experience for every user within your organization.

The Traditional Approach

When you create phishing simulation campaigns, you choose a pretext to send out to the organization. The simulations typically intend to get the user to click on a link, submit credentials, or download malware. The system then tracks the user action, and, if warranted, provides training for improper responses.

Usually everyone in an organization receives the same simulation. More advanced programs might send out messages to different groups of people within the organization. This allows for simulations to be somewhat more tailored to the recipients but requires exponentially more work.

Organizations target users who fall for the phishing simulations more frequently, however they send out messages to everyone else with the same frequency. This tends to annoy users who do not fall for the typical phishing messages, and has little impact in improving awareness for the majority of users. Using an analogy, it is like trying to teach all students in the same high school the same basic math course, over and over again.

The Hoxhunt Approach

Hoxhunt takes a unique approach. Using artificial intelligence, Hoxhunt can tailor phishing education to each individual user. After an organization provides the platform with user information and the appropriate access, the system then sends out messages. Based on the responses of each user, the system itself then determines the appropriate frequency and simulations moving forward.

Should a user fall for the simulation, they receive the designated training, and the next phishing messages are of similar sophistication. However, when users do not fall for the phishing simulation, the system can then raise the sophistication of future messages. This has the impact of improving learning by making future simulations and any resulting training more advanced. Similarly, if a user consistently demonstrates awareness, they receive fewer simulations.

Should a user begin to fall victim to the simulations again, the system can throttle up the simulations to that particular user. This clearly provides for a very personalized learning experience that cannot be achieved through the competition.

The individualized nature of the messages and the training allows for yet another unique feature; customized spear-phishing messages. The Hoxhunt platform allows the tailored messages to appear like they come from another user in the organization. Hoxhunt pulls the name of other users on the system, from within their same department. This simulates the targeted messages sent by more sophisticated attackers.

In short, there is simply no other platform available that allows for this level of phishing customization, automatically tailored to individual users. All of this is accomplished with little administrator input.

Hoxhunt Optimizes Learning

From a learning science perspective, this approach has very distinct advantages. Training needs to be appropriate to target. Training that is too complex will not benefit a novice user. Likewise, training that is too simple for a person with more expertise will not only be waste of time, it will also be likely to aggravate the student.

In the case of phishing, hitting less experienced users with advanced attacks will lead to frustration, and will overwhelm the user. On the other hand, if you send out basic phishing messages to accommodate the less knowledgeable users, advanced users will never improve their expertise.

The Hoxhunt approach provides for users of all knowledge levels to increase their expertise at a reasonable and steady pace. No other tool out there allows for this customized learning experience. Having used most major phishing platforms, we have found that there are few distinguishing factors them. However, the Hoxhunt machine learning approach to customize the phishing simulation experience for each individual user. This is an incredibly unique and valuable feature, which means that all organizations should consider the Hoxhunt solution for their phishing simulations needs.

Written by

Ira Winkler

President, Secure Mentem

Ira Winkler, CISSP, is President of Secure Mentem and Author of Advanced Persistent Security. He is considered one of the world's most influential security professionals and was named "The Awareness Crusader" by CSO magazine in receiving their CSO COMPASS Award. He has designed and implemented and supported security awareness programs at organizations of all sizes, in all industries, around the world.