CyberHoot Press Release

CyberHoot Phish Testing Announcement

FOR IMMEDIATE RELEASE

Portsmouth, NH – March 2022 – CyberHoot has released a new Phish Testing capability within its cybersecurity awareness platform. Our newest module makes it exponentially easier to test your user's phishing skills by eliminating set up and troubleshooting of Allow-Listing, X-Headers, Chrome Intercepts (red screen of death) and clutter/spam/junk folder filing issues. CyberHoot's new feature sends a Phish Test assignment to a user's inbox the same way CyberHoot sends its training assignments. Users are prompted to open the phishing assignment and work through a guided phishing test. The learning opportunities are profound as CyberHoot provides in the moment feedback and instruction on what users should be looking for to identify and confirm a phishing attack.

Module Features

- Users are randomly shown *a combination of phishing and legitimate vendor emails.* They are then prompted to investigate and determine 'Safe' or 'Phishy' aspects of each part of an email across 7 tell-tail signs that help identify a phished attack including:
    - Sender (orders@rnicrosoft.com) Typosquatted domains
    - Subject Line (Order Confirmation) Urgency, unexpectedness, spelling etc…!
    - Greeting (Valued Customer) Lack of a personal greeting
    - Spelling, Punctuation, and Grammar (Youre accounts, been hacked!) Obvious
    - Urgency (Change your password ASAP or you'll be fined!)
    - Link (https://z00m.com/l0gin) Match vendor, obfuscated, or other concerns?
    - Attachment (Instructions.exe; .bat; .docm) Dangerous file types explained
- CyberHoot has over 100+ different vendor emails from around the world. Each database entry contains a legitimate email and fake/phishing email from each vendor. We randomize what a trainee receives ensuring they need to carefully examine each of the 7 areas above.
- We evaluate users using three different levels of difficulty: Easy (prompts), Moderate (prompts), Difficult (no prompts)

CyberHoot CEO and Co-Founder Craig Taylor stated:

Phish testing has become nearly impossible for most MSP's when done the traditional way. It is flawed in so many ways that CyberHoot has now addressed. For example: *Did my user get the phishing email in their inbox? If so, how do I know they saw the phishing email and ignored or deleted it?* With our new module, you save enormous time and money with setup, and you get better outcomes with end users, and you are guaranteed to test every employee you have.

Become More Aware to Become More Secure.

CONTACT INFORMATION:

For a Demonstration of this Module: **Sales@cyberhoot.com**

Vendor Phish Test Requests

: **support@cyberhoot.com**

Sign up today at: **CyberHoot.com**