WE MAKE CYBER SIMPLE

PHISHING – STILL INCREDIBLY SUCCESSFUL

There is so much information about phishing you might think that it wouldn't succeed anymore. But the latest research from CISA, the Computer Security and Infrastructure Security Agency, shows how successful phishing still is.

- In 8 out of 10 organizations at least one person took the bait
- Ten percent of the emails sent by CISA succeeded in getting someone to click on a malicious link or download a malicious attachment
- Only 13% of employees reported receiving the phishing emails or texts to management. Without knowing about them, IT and executives cannot take action.

In my view, phishing is still so successful because of a few things:

- People are often over worked and rushed
- IT teams are stretched very thin and have tight budgets
- Cybercriminals are very good at sending emails that look real and prompt quick action
- Cybercriminal techniques get past many of the protections and tools
- People are just people who will click links that come from apparently authorized people or that look interesting

All these things combine into a perfect storm of danger and damage. With employees under pressure to complete their work, they don't take the time to examine and confirm if an email or text is real.

To make these emails believable, cybercriminals pose as company executives, colleagues, acquaintances, reputable organizations, government representatives, or others that appear authorized to request this information.

Protection today uses complex tools to try and keep the phishing emails out and away from users. But in CISA's test, 70% of phishing emails and bad attachments got through. The high percentage of people that still get caught shows that tools alone aren't enough. Education and training are essential. Cybercriminals continually find new ways to get past the technology protections. People need to know how to spot suspicious messages and who to report it to. Rewarding people who do report it promptly, reinforces that behavior.

Once that link is clicked or the attachment downloaded, the cybercriminal "owns" the user's computer. From there the malware is spread throughout the organization. Depending on the type of malware, it may be sending credentials or other private information back to the cybercriminals, or it may be ransomware that will be activated once it infects enough of the infrastructure.

Regardless of the type it is very damaging. Teaching people to recognize phishing and not click is the best way to prevent damage.

The full CISA report can be found here.

Are you ready to get serious about protecting your assets and your company? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.