

March Newsletter



BLOG: What is Honeypot Cyber Security and Why Do You Need It?

What is a Honeypot? How do they work and why should I care about them? Honeypots are fake systems that act as a decoy to distract hackers from your real system and they can cause big trouble for businesses of all sizes. Read our blog to learn about the types of Honeypots and how you can help prevent them from impacting your workplace.

[READ BLOG](#)



Remote Workforce Training Courses Promote Good Cyber Hygiene

With more companies moving to remote or hybrid-remote work models for their employees, it's important that security awareness training keeps pace. That's why we offer Security Awareness Training for the Remote Workforce as part of our solution set. How are your remote teams' unique security awareness training needs being addressed?

[LEARN MORE](#)

When Stories Turn Into Deceptions

A con usually starts with a story. In a typical scenario, a criminal picks a mark, shares a plausible story, and then waits for the chosen mark to fall for the line. Once the bait is picked up, the criminal steals the loot. Cybersecurity is no different. A recent blog published by Inspired eLearning introduces us to pretexting.

Pretexting is a social engineering technique where hackers manipulate people into revealing confidential information after gaining their trust. How did they gain this trust? They tell a story.



This article explains what pretexting is. It reveals common patterns to watch out for and provides six real life examples to show you how pretexting works in the real world. It concludes with three proven strategies to help you overcome pretexting.

The takeaway? Dedicated cyber security awareness training on a regular basis through a world-class training platform like Inspired eLearning can help all of us to spot the schemes attackers are using no matter how creative they are!

Read the full article here: [What is Pretexting in Cybersecurity?](#)

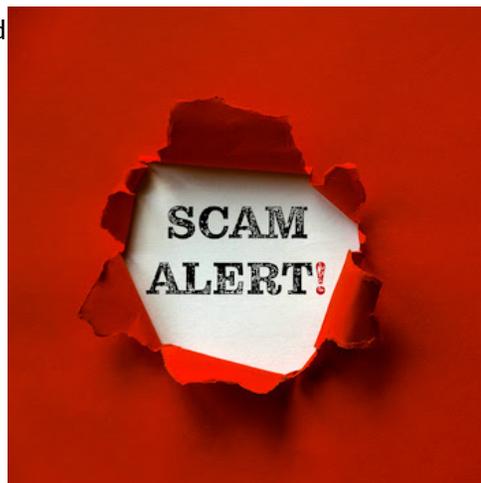
READ THE ARTICLE

FBI Reports Surge in Business Email Compromise - Are You Protected?

FBI Reports Surge in Business Email Compromise - Are You Protected? With the increase in people working from home as well as hybrid working practices, the FBI has seen a large jump in the number of Business Email Compromise (BEC) scams over the past two years. Scammers are using virtual meeting applications to instruct victims to send unauthorized transfers of funds to fraudulent accounts.

If your business is worried about BEC, you need to ensure that you are investing in technology, training and tools to keep your network, users and data safe. Take a look at [VIPRE Edge Defense](#)

- a full security suite which does exactly that - advanced email security and encryption, year-round user training and phishing simulations, as well as human-led DLP.



[LEARN MORE](#)

Keep Your Networks and Your Data Safe with Automated Vulnerability and Patch Management

A key area of cybersecurity defense that is often overlooked is Vulnerability and Patch Management, but we have a simple solution for that - [VIPRE Endpoint Cloud](#). By easily identifying and highlighting vulnerabilities in the management console, IT admins can apply recommended patches instantly, keeping their networks, data and people safe from out of date software exploitation.

[Contact](#) your Inspired eLearning account manager today and find out how you can expand the protection of your networks.

[DOWNLOAD DATASHEET](#)



Proactively Addressing the Human Component of Data Security

Compliance and risk management solutions like the award-winning Inspired eLearning programs continue to be key in protecting an expanding digital footprint against emerging threats.

According to the Gartner “[Top Security and Risk Management Trends for 2022](#)” report, “Human error continues to be a factor in many data breaches, demonstrating that traditional approaches to security awareness training are ineffective. Progressive organizations are investing in holistic security behavior and culture programs (SBCPs) fostering new ways of thinking and embedding new behavior with the intent to provoke more secure ways of working across the organization.”

[Let](#) us know how we can help keep your organization's security awareness top of mind.

[READ THE REPORT](#)

Connect with us:



© 2022 Inspired eLearning, LLC. All rights reserved.

info@inspiredelearning.com | 800.631.2078

[4630 N Loop 1604 W, Suite 401](#)

[San Antonio, TX 78249 USA](#)

[Privacy Notice](#) | [Email Preferences](#)