



Cyber Threats to Schools & Municipalities

SERVICES AVAILABLE

Dellicker Strategies has solutions & services to help public organizations get their cybersecurity under control.

ESSENTIALS PACKAGE

- Security awareness training
- Network vulnerability scan
- Incident response retainer
- Program development

SUSTAINMENT PACKAGE

- Essentials Package plus:
- Additional training seats
- 2nd vulnerability scan
- More tech & program support

COMPREHENSIVE PACKAGE

- Sustainment Package plus:
- Penetration testing
- Advanced endpoint protection
- Additional technical capabilities

Dellicker's delivery partners include Candoris Technologies, and KnowBe4.

Contact us today for a free cybersecurity assessment:
Info@dellicker.com

Prepared by Aliyah Vinas

Spear-Phishing

Social engineering attacks are getting more sophisticated and more dangerous as criminals find new ways to trick unsuspecting email users.

What is spear-phishing?

Phishing is when a criminal sends out bulk emails to a group of people hoping that some of them will be fooled and click on a bad link. Spear-phishing is similar, except the criminal uses more personalized information about his victims to get them to give up their credentials. Often, spear-phishing involves directly targeting someone that has special access to certain data. Sometimes, a researched script may be embedded into the email that incorporates the personalized interests of the victim.

Who are the perpetrators?

Spear-phishing usually is done by trained criminals out to make money.

How do they operate?

Hackers tend to gather a user's preferences long before sending out a spear-phishing email. They want to learn about where their victim shops, eats, what websites they visit, and where they conduct business. Then the criminal uses that personal information to generate a compelling email that prompts a response from the victim.

Stranger Danger

Most of successful data breaches start with a spear-phishing attack. Once an attacker enters system, keylogging, screen-logging, webcam, and microphone recorders can be enabled without the owner being aware.

Taking Action

Be careful about exposing employees' email addresses on company websites. Make sure employees have proper training against social engineering attacks. Think before you click!

*Source: KnowBe4. <https://www.knowbe4.com/spear-phishing/>

Contact Dellicker Strategies:

8766 Bittners Ct, Lehigh Valley, PA 18053 | P: 484-788-1221 | E: info@dellicker.com | www.dellicker.com