Social Engineering

Protect Your Network From Cyber Criminals

Cyber criminals have found that the easiest way to gain access to a financial institution's network is through social engineering.

CRIMINALS GAIN ACCESS

In-Person | By Phone | Digital Devices & Networks

In-person attacks take several forms, the most common being impersonation of service technicians to gain access to an institution's facilities and/or network. Another common method includes leaving a device (flash drive) behind in hopes that an employee will attempt to use the infected device.

Phone attacks are becoming more common as companies increase their network security. Attackers call employees pretending to be company executives needing a funds transfer, service technicians needing network access, angry customers, charities, or business partners that require information.

Digital attacks can take several forms, the most common being phishing attacks. Other methods include infecting trusted websites of regulators or business partners and emails from known email accounts.

THE COST OF CYBER CRIME

Source: SmartFile

28% WILL EXPERIENCE A DATA BREACH IN THE NEXT TWO YEARS
77% OF ATTACKS ARE PHISHING
3.8M IS THE AVERAGE COST OF A BREACH
4.6M IS THE ESTIMATE NUMBER OF PHONE HACKS
90% OF DATA BREACHES COULD HAVE BEEN PREVENTED

TESTING TYPES

We perform social engineering tests to determine the effectiveness of employee training, internal controls, and processes in preventing social engineering attacks against an institution. We perform testing using various methodologies, including:

- Dumpster diving
- On-site visits
- Phishing & Vishing
- Pretexting

417-882-4300 | info@kpmcpa.com
www.kpmcpa.com | #KPMCPAs
1445 E. Republic Road | Springfield, MO 65804

KPM
CPAS & ADVISORS

Let's Connect

Contact Us Today To Speak With Our Advisors