Cybercrime has become a multi-billion dollar industry. What we've found is that no industry or size of company is safe. The good news is that cybersecurity technologies have evolved to effectively protect end users and mitigate costly threats such as ransomware and phishing. Companies must practice defense-in-depth strategies and have buy-in at all levels. Untrained employees remain an organization's greatest vulnerability, so a strong cybersecurity awareness program is key, in addition to keeping their data protected and recoverable with proactive technology safeguards."

JEFF LAURIA
VP OF TECHNOLOGY

GET IN TOUCH WITH US

PHONE
(888) 642 - 6484

WEB
https://www.icorps.com/cybersecurity

CYBERSECURITY

THE BIGGEST THREATS

Presented by

iCorps
TECHNOLOGIES

THREATS

Ransomware

Ransomware is a malicious software that encrypts files so you can't use them until you pay a sum of money, the ransom. It is growing at a rate of 350% and is expected to be exceed $5 billion in costs to businesses by 2018.

Mass Phishing

Mass phishing email attacks are sent to large groups with the intent of obtaining personal information or installing malware on the user's computer. More than 30% of these emails are opened and more that 400,000 fraudulent sites are visited each month.

Targeted Phishing

Targeted, or spear, phishing is electronic communication targeted towards an individual or department within an organization that appears to be from a trusted source. These attacks steal data, compromise credentials, or install malware on the target's computer.

Business Email Compromise

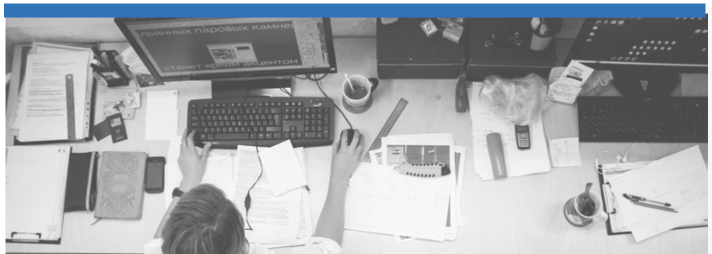
Also known as "whaling," these scams are a form of financial fraud where spoofed emails are sent to staff by scammers pretending to be upper management requesting a large money transfer. Since 2013, over $960 million dollars have been lost by these scams in the United States.

Password Attacks

There are multiple types of password attacks, but all involve obtaining passwords through software, old data, and algorithms. Passwords are obtained to gain access to data. In fact, 63% of data breaches result from hacking weak passwords.

Social Engineering

Social engineering preys on human emotion and vulnerability; the attackers use human-to-human interaction to manipulate the victim to divulge personal information. These attacks target the education industry the most, preying on teachers and students.



SOLUTIONS

1 Assess and Lock Down Your Environment

There are a plethora of affordable tools available to protect your environment from these threats, including identity management services, advanced threat protection, URL protection, web filtering, threat monitoring, data backup, and antivirus monitoring.

2 Implement Secure Cloud Services

Due to high availability and privacy controls, the cloud is an excellent tool for ensuring data recovery and business continuity if files are compromised. Multifactor authentication is an additional tool you can implement to ensure higher security.

3 Educate and Train Employees at All Levels

Insiders are the cause of 90% of security incidents. To avoid this, teach employees how to identify phishing schemes, stress the importance of caution when opening links, and create a culture of security. A strong security awareness training is on going to keep up with today's threats.

4 Have a Cyber Recovery Plan in Place

A cyber recovery and business continuity plan are essential for any proactive company. In the event of a cyber attack, a business continuity plan will provide foolproof data backup and disaster recovery., as well as technical, legal, and PR processes and plans.

5 Patch your Systems

Leverage a solution or managed services provider to keep your on-premises devices patched and up to date with the latest software updates.