BLOG

Hackers get the headlines, but social engineers get the data

By Rob Rosenzweig, National Cyber Risk Practice Leader

Nov 13, 2018

Not a day goes by without a data breach of some type making headlines. Most of those headlines are covering breaches perpetrated by so-called black hat hackers exploiting a technical vulnerability. While far less exciting, the vast majority of incidents exploit human vulnerabilities by crafting extremely targeted so-called social engineering emails to induce recipients to offer up their account credentials.

These attacks can be costly if email accounts contain personal identifiable information and even if they don't hackers are often able to gather additional information that allows them to move laterally and take over other accounts or further target others within an organization.

Like most things related to cyberattacks, forewarned is forearmed. Given the pervasiveness of Microsoft Office 365, and in light of these type of attacks, it's important to understand best practices, known issues and how recent changes in this application suite - to user activity logs availability, for instance - can be the difference between a minor incident and a long, drawn out, expensive catastrophic event.

So, with one of our preferred forensic partners, Crypsis, we're making available a one-sheet outlining some key cyber security best practices for Office 365 to help prevent social engineering incidents and to minimize their financial impact. Download it by clicking here.

Want to go deeper and learn more about the threats of social engineering attacks, how you're prepared – or not – to handle them and whether your coverage will be there when you need help recovering? Feel free to connect with us today cyber@risk-strategies.com

TAGS:
Cyber Liability