COMPUTERWORLD

Print Article ☒ Close Window

How hackers find your weak spots

A look at some of the ways hackers use social networking tools to gain access to victims' systems

Mary Brandel

October 19, 2009 (Computerworld)

While there are an infinite number of social engineering exploits, typical ones include the following:

Stealing passwords: In this common maneuver, the hacker uses information from a social networking profile to guess a victim's password reminder question. This technique was used to hack Twitter and break into Sarah Palin's e-mail.

Friending: In this scenario, a hacker gains the trust of an individual or group and then gets them to click on links or attachments that contain malware that introduces a threat, such as the ability to exploit a weakness in a corporate system. For example, says Netragard CTO Adriel Desautels, he might strike up an online conversation about fishing and then send a photo of a boat he's thinking of buying.

Impersonation/social network squatting: In this case, the hacker tweets you, friends you or otherwise contacts you online using the name of someone you know. Then he asks you to do him a favor, like sending him a spreadsheet or giving him data from "the office." "Anything you see on a computer system can be spoofed or manipulated or augmented by a hacker," says Desautels.

Posing as an insider: Imagine all the information you could extract from an unknowing employee if you posed as an IT help desk worker or contractor. "Roughly 90% of the people we've successfully exploited during [vulnerability assessments for clients] trusted us because they thought we worked for the same company as them," Desautels says.

On the Netragard blog, he describes an exploit in which a Netragard worker posed as a contractor, befriended a group of the client's workers and set up a successful phishing scheme through which he gleaned employee credentials, eventually gaining entry to the entire corporate infrastructure.

Next: BT's Web 2.0 security strategy

Related Links

- Scams, spams & shams
- Hijacked Web sites attack visitors
- Zappos gets savvy with social media
- Baited and duped on Facebook
- How hackers find weak spots
- BT's Web 2.0 security strategy
- Public cloud vs. internal social networks
- IT forensic experts find lucrative work
- Profile of IT forensics professional Rob Lee
- Opinion: Web 2.0 security depends on users