HINSHAW

Personal Information is being used in a New Cyber Extortion Scam

Privacy, Cyber & AI Decoded Alert | 2 min read
Aug 1, 2018

Download a PDF of the alert

Risk Management Question: Personal information about you is knowingly or unwittingly circulated in cyberspace every day. A new cyber extortion scam involves emails claiming to have embarrassing or incriminating information about the recipient and demanding payment. The sender references just enough personal information to make the recipient pause before hitting the delete button. What should you and your firm do if you receive such a threat?

The Issue: The FBI is warning of a scam in which cyber criminals claim to have confidential or embarrassing information about you that will be released unless a ransom (typically Bitcoin) is paid. The latest version adds a new twist by including a reference to a password in the opening sentence that may in fact be an old password that you previously used. Hackers are able to acquire these passwords through online forums, data breaches of social media providers (LinkedIn, Yahoo, etc.) or through internet research. A number of law firms recently reported receiving extortion attempts similar to the one uploaded here (complete with the original misspellings and grammatical errors).

While the email is a crude attempt at extortion, the sender did enough research to guess a password that the recipient used in the past for an account, in this case a child's name. While this adds to the "creepiness" of the attempt, again, it is important to remember that it does not take a lot of research to find the names of our children, parents and other family members on the internet. Social media sites love posting harmless or cute looking pictures as part of a poll to ask questions like the name of your first pet.

Risk Management Solutions:

If you receive a threatening email:

- Immediately report it to your firm's IT department to be investigated. The sender of the email should be blocked and the extortion attempt reported to the FBI cyber-crimes unit.

- Never open attachments that claim to show your confidential information, do not reply, and never send money—in any form. Responding to these emails will only increase the likelihood of ongoing harassment.

Take precautions to prevent the use of your personal information and passwords:

- It is important to stop and think before responding to requests for, or posting, personal information, and to exercise caution before giving away information about ourselves, especially information that is used in common security questions.
- Never use the name of a family member (or a pet for that matter) in any password, and with the prevalence of dictionary attacks, don't use words that appear in a dictionary. Think passphrases not passwords, and the longer the phrase the better, *e.g.* IhateMyFir$tex! would be a strong password and one that might be easily remembered. Think of something memorable for your passphrase.
- Never use the same password for access to more than one account, site or application, and never use your firm or company password for access to any other account, site or application. Reusing passwords across multiple sites puts them all at risk if one site is compromised.
- A helpful site, https://haveibeenpwned.com/ can assist in identifying when personal accounts have been compromised due to data breach.

Additional recommendations:

- Do not communicate with cyber criminals.
- Be sure that the security settings for your online accounts are turned on and set at the highest level of protection.
- Always use two-factor authentication when available.
- Stay vigilant. Emails and text messages requesting personal information and passwords may appear to be legitimate, but never supply that information.

Always think before you click.

Related People

Steven M. Puiszis

Partner

312-704-3243