May 16, 2018

Cyber Alert – Dual Factor Authentication Can Be Hacked By Phishing

Risk Management Question: Dual factor authentication greatly increases your online security, but it is no panacea. Dual factor authentication can be compromised through social engineering and phishing exploits. What can law firms and their employees do to identify and avoid phishing emails attempts to defeat the protection provided by dual factor authentication?

The Issue: Dual factor authentication increases online security because it adds an additional step or layer of protection when logging in to gain account access. However, accounts protected by dual factor authentication can still be hacked via phishing emails. Included below is a link to a video from Kevin Mitnick, a computer security consultant, showing how an account protected by dual factor authentication can be compromised. It's called "session cookie hijacking."

The video demonstrates how an attack can occur with a phishing email that appears to be sent by a LinkedIn member asking the victim to connect. In the video, Mr. Mitnick notes that while the email looks legit, if you carefully review it, you will find that the return email address is incorrect. When the victim clicks on the "interested" button, malware is launched onto the victim's computer. The victim is taken to the real LinkedIn site where login information is required to complete the process, which includes LinkedIn sending a text message (the dual factor) with the access code to the victim's phone. However, the malware is capturing the victim's email address, password and session cookie, which will allow the hacker to later access the victim's account directly and bypass the dual factor authentication portion of the sign-in process. While the video uses LinkedIn, the same attack can be made to any online account.

When you watch the video you may be surprised to see how easy it is to hack dual factor authentication if you are phished: https://is.gd/HYFhpR

This is not meant to suggest that lawyers shouldn't use dual factor authentication – it should be used whenever it's offered for remote access to any online account. However, even this protection can be hacked if you are not careful with how you handle email attachments and links. Always think before you click.

Risk Management Solution: Remember these three essential phishing rules:

1. Never click on a link or an attachment from someone you don't know;
2. Never click on a link or an attachment you were not expecting to receive, even if you know the sender. Call the person first to confirm that person (rather than a hacker) sent you the email before you click on anything; and

3. Finally, if you forget the first two rules and click on a link or an attachment and either a zip file or dialog box is presented which asks you to supply additional information or a password, enable a later software version, or open the zip file, stop immediately and close out. Then call your firm's IT department to have a scan run on your computer.

Another way to mitigate this exploit is to avoid using the link provided in the email and instead go to the site directly. This may not be foolproof, but it helps reduce session cookie hijacking.

Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com

Anthony E. Davis
212-471-1100
adavis@hinshawlaw.com

Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com

Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com