HINSHAW

Alerts

'Tis the Season for Spoofed Greetings

November 13, 2019
Cyber Alert

Download a PDF of the alert

Risk Management Question

What steps can law firms take to guard against greeting e-card scams?

The Issue

Winter is coming, and along with it, your employees may start receiving holiday e-cards on their work computers. Malicious e-cards are an increasingly common and successful way fraudsters trick you into letting your defenses down during the holiday season. Rather than bringing you joy, clicking the link to the e-card instead leads you down a path festooned with malware, and ultimately to a cyber breach.

There are a number of ways a clever trickster can make a fake email appear legitimate. For example, they can use a program to input captured personal information—such as a known friend's name—and embed that into the email to you, while hoping you won't notice that the sender's email does not match the displayed name.

Most legitimate e-card messages will include a confirmation code which allows you to open the e-card without clicking on a link. Simply open a new window and go directly to the greeting card's website. Then, enter your email address and the confirmation code to receive your season's greetings.

Risk Management Solutions

Remind employees to take these steps to try and avoid greeting card scams:

- Be cautious of emails from a "friend" or "secret admirer" or even a sender that may appear authentic like "ecard@greetings.com"
- Do not trust the displayed name in the sender field; check the sender's actual email address to confirm whether the message is from a trusted source
- Delete e-cards that include a link or attachment that ends with ".exe," which signifies an attachment that wants to run a script and could download a nasty virus

Attorneys

Steven M. Puiszis

Service Areas

Law Firm Cyber Alerts

Lawyers for the Profession®

- Do not click links in the email, even if the e-card looks legitimate
- If you receive an e-card, go directly to the company's website to access the card using the confirmation number in the email you received

These same tips apply to e-gift cards. Never click the link in the email. Instead, go to the known and trusted company website and enter the gift code there. Above all else, educate your employees on a regular basis about how to spot and avoid new spoofing techniques.

Happy Holidays from Hinshaw! And remember, always think before you click.