"Bonus Payment" Phishing Emails Are Seeking New Ransomware Victims

February 3, 2022
Law Firm Cyber Alerts

Risk Management Question

How can employees mitigate the risk of falling for phishing scams purportedly sent by their company's HR department?

The Issue

Scammers often know just the right thing to say to pique an employee's interest and lower their guard. Recently, a phishing campaign has re-emerged where bad actors send bogus emails that appear to be sent by the employer's HR department detailing important information regarding bonus payments. Even more convincingly, these emails often come from legitimate-looking domains and URLs.

These phishing attempts usually contain a fake attachment which, when clicked, asks the user to enter their email and password in order to access their bonus information. This type of scam, called "credential phishing," works by preying on human trust and distraction: employees are more likely to move quickly and ignore spelling and grammar mistakes when money is involved.

Once entered, phishers can use these credentials to subject the company to ransomware, remote access tools (RAT), keystroke logging malware, and desktop image capturing malware. Beyond the resulting damage to the business, the hacked credentials might also be sold on the dark web, leading to personal identity theft for the employee.

Risk Management Solutions

Follow these practical tips and share them with your employees to help spot phishing scams:

- Don't ever click on an attachment from someone you don't know, no matter how harmless or tempting the attachment may seem.
- If you receive a link or attachment from someone you know that you weren't expecting to receive, call the sender before opening the link or attachment. Use your company's directory or website to identify their phone number, not the number provided in the unexpected email.

Service Areas

Counselors for the Profession

Cyber Security for Law Firms

Law Firm Cyber Alerts

Lawyers for the Profession®

- Be sure to carefully inspect the email address or domain name of the email sender. Scammers often use domain names or email addresses that are virtually identical to real ones, but with a typo or other nuanced change.
- Don't use the same email and password combination for multiple accounts. This puts your entire online presence at risk if just one login is compromised.
- If your company has one, be sure to look for the "external email" warning on emails. Emails coming from your own company's HR or other departments are internal, and will not have this warning.
- Finally, if you do accidentally click on a phishing attachment or log into what seems like a fake site – stop, close out of the document or webpage, and call your IT department to have a virus scan run on your computer.

Scammers are getting smarter and more creative every day. But if you use your head and think before you click, *you* can outsmart *them*.