The Jaffe Update
Legal News Delivered

A publication of Jaffe Raitt Heuer & Weiss October 7, 2020

PROTECTING YOUR COMPANY FROM VISHING ATTACKS DURING COVID-19

With the increased number of employees working from home and being granted remote access to their company's network during the pandemic, voice phishing or "vishing" has been on the rise. Vishing is a phishing attack executed via phone calls.

In a vishing attack, the criminal calls the employee and pretends to be a co-worker/newly hired co-worker, or service provider of the employer. The goal is to: i) convince the employee to divulge their login credentials over the phone; ii) input their login credentials manually on a dummy site that the criminals set up to mimic the company's corporate email or VPN portal (the criminals simultaneously enter the login information on the real login page and the employee authenticates through his/her dual authentication app); or iii) gain information about the company to use to make himself sound credible when calling another employee. Criminals are able to learn the company's internal processes and lingo through social media sites and through calls to various employees that may divulge bits of information about the company, which can then be used to sound credible when calling another employee. The goal of the attacks is to gain access to the company's internal data bases and tools in order to mine financial data, proprietary information, trade secrets, and personal data of the employees and customers of a company.

Things you can do to reduce the likelihood that your company will become victim of a vishing attack include:

- **Make your employees aware of the existence of vishing attacks.**
- Restrict VPN connects to company owned devices.
- Restrict the hours in which VPN access is available to employees.
- Monitor domains created that are similar to your company's domain.
- Limit employee access to the company's network based upon the need of the employee to perform his/her job function.
- Implement formalized authentication processes for employee-to-employee telephone communications, where a second authentication factor is used before discussing potentially sensitive information.
- Instruct employees to limit the personal information posted on social media sites concerning the company.
-

Please contact us if you have any questions.

Jon Sriro
313.800.6502
jsriro@jaffelaw.com

Jaffe
JAFFE RAITT HEUER & WEISS