FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

Legal Update

February 2017

DON'T CLICK THAT: PROTECTING AGAINST EMAIL SCAMS AND MALWARE

By Peter T. Berk

To: H. Walker- HR From: J. Jones – CFO Subject: Tax Requirements Please send me .pdf copies of all of our W-2 forms. I need them for our auditors. Thanks.	To: B. Smith – Controller From: R. White –CEO Subject: Wire Transfer – URGENT Please wire $17,532.67 to our vendor, ACME Scams Co., immediately so we can have our order shipped on time. The account information is attached.

These are just two examples of types of emails that scammers have used to target companies. In these examples, and others, the offenders use social engineering, publicly available information, and other methods to learn a company's email form, the identity of its key employees, vendors and clients, and work schedules, and how employees communicate with each other. This helps the scammers make the emails look authentic and increases the chances of the recipient complying with an otherwise unusual request. Other questionable emails with links and attachments include: summonses for court cases; complaints about invoices; security alerts; social media alerts; and industry conferences and conventions.

As scammers become more and more creative in their tactics, and more advanced in making their emails look legitimate, companies must be vigilant and proactive to protect themselves. If they don't, they risk losing money, losing company secrets, and entire servers being encrypted until they pay a ransom. Here are some areas in which companies can take simple, preventive measures to limit their risk:

1. Technology: Having appropriate network security (system security checks, anti-virus software, firewalls, *etc*.) that is frequently and updated can limit the risk of delivery of questionable emails, block questionable attachments, and help prevent intrusions seeking information.
2. Policies and Procedures: Having proper policies about employee use of technology and the internet is important, but company policies and procedures should also address how to handle and store sensitive information (trade secrets, financial information or personally identifiable information), as well rules for the authorization of payments and financial transactions.
3. Training: Training employees is crucial. Employees should not only be advised of the company's policies and abide by them, but also should be made aware of common scams and how to avoid being fooled (how to spot questionable emails or links, how to handle strange attachments, *etc*.).
4. Preparedness: Working with your legal advisors and key stakeholders is especially important for identifying risks, conducting regular audits of your systems and practices, and creating a response plan, which will help keep your company ahead of the game.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or contact Peter T. Berk 312.701.6870 pberk@fvldlaw.com, Twitter: @BerkPeter, LinkedIn: www.linkedin.com/in/pberk, or your regular FVLD contact.

FVLD®