HOW OUR EMAIL SYSTEM GOT HACKED

Recently, one of our employees received an email from a valued client. The email said that important information was attached and to open the attached weblink to retrieve it. The employee opened the weblink and found a Google sign in page. The employee was asked to sign into their Google account to get the promised information. The employee did. Next, a message stated that there was a problem and the link couldn't be opened at this time.

Two days later, my banker called me to confirm whether I wanted to wire $47,550 to an account in Baltimore for the purchase of a manufactured home. My banker was confirming an email request from what she thought was my office to do just that. We had sent no such email request. And we stopped the wire transfer from happening.

Here's what happened. Our client's email system was hacked. The thief was then able to acquire their contacts and replicate their email and send an email to us that appeared to be from our client. When our employee opened the link, and complete the Google page, they were entering their Google password into the thief's fake Google look- a-like page. With this information, the thief was able to open our employee's email account and see who they talked to and what subjects they addressed. Thereafter, the thief emailed the bank employee, who we regularly communicated with, and asked for the wire transfer using names and phrases we often use. The thief specifically asked our banker not to follow up with a confirmation call as we were busy and out of the office. The thief's email to our banker looked just like it had come from us. (This is basically how the Democratic National Convention and Hillary Clinton's team were backed in 2016.)

One thing we'd done right was to have previously visited with our bank about wire transfer safeguards. We'd asked the bank to confirm by phone any wire transfer requests. In addition, we invested in a "Cyber Liability Insurance Policy" two years ago that would have helped had this situation gotten worse. This policy protects us from private data loss, system damage due to hackers, liability caused due to hackers, copyright infringement, etc.

To reduce our future risk, we:

1) Trained our employees not to open weblinks in an email purporting to have documents accessible in it and to only open attached files ending in .jpg or .pdf;
2) Now review our online bank transactions daily for unapproved activity;
3) Trained our employees to never update or authenticate account information pursuant to an email request;
4) Advised our bank that all wire transfers must be requested in person;
5) Now use public WIFI systems sparingly, and never access sensitive information while on WIFI. Employees with unlimited mobile data plans will use them exclusively; and
6) Adopted a new email protocol which requires two passwords if previously unauthorized locations or devices try to access the system.

STAY ON YOUR TOES…
The Barbarians (and Russians)
are at your internet portal!

Kurt D. Kelley, J.D.
President, Mobile Insurance
Kurt@MobileAgency.com
www.mobileagency.com

President of Mobile Insurance, an agency specializing in insurance for manufactured home communities and retailers. Named top commercial insurance agency by American Modern Insurance Group. Member of numerous insurance companies' policy development and advisory teams. One of largest manufactured home specialty agencies in the country.
2017- Present Founder and Publisher of the Manufactured Housing Review, an industry publication dedicated to Manufactured Home Industry professionals. www.manufacturedhousingreview.com

MOBILE INSURANCE
800.458.4320
www.MobileAgency.com