Gallagher&Kennedy
Lawyers. When Results Matter.

Church & Ministry Law Newsletter
April 2017

A Treacherous, New Twist on an Old Scam

Remember when you received an email from a hapless Nigerian Prince? In this classic scam the sender claimed to be a member of a royal family or a government official.

In a personal encounter with one of these emails, I had a difficult time convincing an elderly Swedish Pastor client NOT to agree to help the Prince transfer millions of dollars out of Nigeria. He planned to use the "fee" to aid missionaries in Africa. The retired pastor insisted that we meet on Saturday morning because the message was marked "urgent, private".

The Treacherous, New Twist!

The scammer impersonates the victim's boss in a legitimate sounding email asking, "Hi, are you in today?" The scammer then requests copies of sensitive information such as tax forms, employee lists and social security numbers. Sometimes the scammer will send a series of innocent emails before asking for the sensitive information.

Upon receiving the victim's sensitive information, the scammer sells it on the open market for between $4 and $20, as indicated by Brian Krebs, a well-known computer security blogger, in a recent post. Some cases have even resulted in a loss of all the cash in the victim's bank accounts.

In a variation, the scammer impersonates an executive and emails the company's payroll department or comptroller requesting a wire transfer into a particular account.

Take This One Seriously!!

"*This is one of the most dangerous email phishing scams we've seen in a long time*," IRS Commissioner John Koskinen said recently. "Although not tax related, the wire transfer scam is being coupled with the W-2 email scam, and some companies have lost both employees' W-2s and thousands of dollars." There have been hundreds of victims of the W-2 phishing scams, which started in February of last year.

Your organization—regardless of industry, size, or location—is not immune. The scammer's targets include nonprofits, schools, hospitals and restaurant chains. The FBI estimates that losses could reach $3.1 billion from 22,000 victims.

How to Respond if You are a Victim

If your organization falls prey to a W-2 scam, send the malicious email to phishing@irs.gov and place "W2 Scam" in the subject line. Next, file a complaint with the FBI's Internet Crime Complaint Center (IC3).

If you are an employee whose W-2 forms are stolen, check out the actions recommended by the Federal Trade Commission at www.identitytheft.gov or the IRS at www.irs.gov/identitytheft. If you are an employee whose tax returns are rejected because of a duplicate Social Security number, consult your CPA and an attorney and immediately file a Form 14039 Identify Theft Affidavit.

Robert Erven Brown, Shareholder
bob.brown@gknet.com
Office: 602-530-8023
Cell: 602-740-1032