attacker may send the target an email that appears to be from someone they ...

**Jim Boomer** • Jun. 09, 2016


**From the June 2016 Issue.**

We've all received the email. A Nigerian prince wants you to help him move money into the United States. In return, you'll get to keep a piece of the fortune. With typos and grammatical errors aplenty, most (but not all) are savvy enough to recognize the scam and hit delete. Unfortunately, the criminals are getting much more sophisticated and personal in their tactics and setting their sights on higher profile

targets. These new attacks are going after the “big fish” or in security lingo, they are



What makes this trend so scary is the level of sophistication that recent attacks are achieving. The personal, one-off nature also makes them more difficult for IT to detect than the traditional phishing emails where hundreds of versions of the same message flood the email server. The criminals are doing their research including studying communication styles to make the messages look real. Some even include closely held information and the names of individuals expected to be involved in the exchange.

## Making It Real

Over the last month, we have facilitated almost 100 mid- to large-sized CPA firms in our various peer communities and heard too many stories about these types of attacks. Let me give you a couple examples to make it real.

**Example 1:** The CFO of one firm recently received an email from the managing partner asking her to wire money to a client’s account. The email showed up as a legitimate email address and was written in the exact tone and words used in countless previous exchanges between the two. The CFO did as she had been instructed and contacted the bank to wire the funds. Fortunately, she also cc’d the managing partner and it was caught before the firm was out more than $30,000.

**Example 2:** This one was a personal attack and, unfortunately, did not end as positive. In this attack, an individual was in the process of helping his son buy his first house. He was expecting the final numbers and had an estimate of what to expect. Within the timeframe expected, he received a spoofed email from the mortgage company with an amount very similar to the estimate to wire to the escrow account. The email used the company’s header and appeared to be from the person with which this individual had been corresponding. It also made mention of and appeared to copy other legitimate people involved in the transaction. Ultimately, the funds were transferred and he was out $67,000.

## What You Can Do to Protect Yourself



personal, financial or sensitive data, make it part of the mindset to independently confirm.

2. ***Conduct your own penetration and social engineering testing*** – Whether you hire an outside party or have internal resources conduct the test, just do it. The initial test will provide you a baseline of how savvy your team is on these scams. And, subsequent testing will show if you're making improvements.
3. ***Use common sense with the information you put in the public domain*** – Train your team to limit the types of information they put on social media and other publicly accessible sites. In general, be sensible about publicly providing information that could be used to impersonate you. And don't trust every invitation you receive. If you don't know them, it's best to decline. Even if your friends or connections have accepted.
4. ***Build controls into your processes*** – Again, this is important to both your firm and personally. Look at the process for approving wire transfers and sending out other sensitive information. Build in a multi-party approval process to ensure that multiple people are involved. Also talk to your banks and request confirmation of wire transfers over a certain threshold. Especially if they are international.

## Bottom Line

We unfortunately live in a world where criminals are constantly trying to take what we've worked hard to earn. You have to be on alert and skeptical continuously. Education is the foundation to protecting yourself from falling victim to these scams. Through continual security awareness training and monitoring as well as building safeguards into your processes, you can protect yourself and your firm from falling victim to one of these attacks.