The Key to Wire Fraud Prevention: Out-of-Band Authentication

ATTENTION: Members of the procurement, finance, and accounting departments.

If you deal with buying supplies or paying our vendors, you are at risk of getting fraudulent payment instructions that would lead you to send money to someone trying to rob our organization.

To understand what could happen, see the three scenarios to the right.

How do we protect ourselves?

The best and easiest way to protect ourselves is to use **out-of-band authentication**. This means that you should verify any unusual transaction request **through a different mode of communication** than it came through.

It works because it's much hard for an attacker to impersonate someone trusted through two modes than through one.

For instance, if you get an *email* from a vendor, you should *call them* using the number you previously had on file *and confirm* that they sent the email. This is especially true if they are giving you new account information, i.e., asking you to send money to a different account than you've used in the past.

Similarly, if you get an *email from a co-worker* that asks to send money to a new vendor or changes the account information for an existing vendor, *check it out*. Walk over to their workspace, or call them on their extension to confirm.

Remember, you're our first line of defense against fraud.

Scenario 1—Our system has been breached, and someone's email account has been hacked

In this scenario a hacker has gained access to our systems and is able to hijack our email accounts. This means that they have a co-worker's credentials and can be communicating with you without the co-worker having any idea their email is being used. The result is "your co-worker" sending you an email with fraudulent instructions. Often in these cases the attackers will monitor our communications for a while and use information discovered that way to send a more convincing email.

Scenario 2—Vendor's system has been hacked

In this scenario, one of our vendors has been hacked, and the attacker sends you an email from the vendor's account asking you to send money. Like in the first scenario, the email will be from a legitimate account of someone you have communicated with in the past. The attacker will also likely monitor communications and jump in after legitimate emails have been sent back and forth so that it looks like a continuation of your conversation with the vendor.

Scenario 3—Vendor's email is spoofed

This scenario is different than the first two because nobody had been "hacked." Instead, the attacker just makes it look like they are one of our vendors. Attackers are smart, so the email will look similar to what our actual vendor's email would look like. They may copy the logo. The email address will likely be only off by one or two characters. An example is *CEO@company_xyz.com* vs. *CEO@company-xyz.com.*

beazley