BEFORE

(Client's Rough Draft)

Is it safe to open my email?

2012 has proven to be a record year for spear phishing attacks. The volume of spear phishing attempts has been increasing while non targeted spam has started it's slight decline. Even the software giants like IBM and RSA to the small local banks, magazines, schools with limited budgets and big financial organizations, spear phishing is hitting our infrastructure. In one study, I saw that it was something like 65% of worldwide attacks were in North America. Watch out for this one -- of the more interesting layered approaches in spear phishing is the combination of the Linked in/Facebook/public website with a corporate email introduction. I have been noticing the combination of websites, telephone numbers and email to create a pretty convincing spear phish attempt.

What are the similarities? Being in the business of protecting major companies email, I see a lot of spear phishing attempts, and they are getting harder and harder to tell from real emails from companies. There are solutions out there that look for links, but what about telephone numbers, there are solutions out there that look for known types of malware, etc. In my world, everyone uses email. For everything. Nobody uses faxes, and we are so distributed, that email is the way to send purchase orders, invoices, and contract data. If I miss an email that I need, then I am pretty much "out of luck." If I get someone who is spear phishing me and I am looking for something, like a document (and it just happens to be exploiting a excel macro which I have been hearing more and more about) then the zero-day attack puts me in a very dangerous position. Not just me, but because of the backdoor installed through the malware, my whole company can be in danger. This has a real possible big cost and loss of revenue to us.
In Information Week's **10 Security Trends To Watch In 2012** that I read earlier this year, Alan Brill, senior managing director of the cyber security and information assurance division at Kroll, predicted that no one is exempt from attacks. Well, here we are in the second half of 2012, and every day I hear of more attacks. Is malware sniffing and "good intentions" and a reasonable education enough to keep us safe? I don't think so.

The smartest, best secured companies in the world are being hacked, spear phished and attacked. So what to do? Layer security, educate and provide some real world messaging intelligence.
Layered security means take advantage of a Trusted Sender Recognition solution. Update your systems, and get some G2 on what is going on in your environment. When was the last time your company did some email hygiene layer education? I consult with companies all over the country and tell them to take email more seriously. One incident, can put you in the news paper, and … for all the wrong reasons.

After

TrustSphere Blog, posted July 31, 2012

http://www.trustsphere.com/is-it-safe-to-open-my-email-be-wary-of-spear-phishing/

Is it safe to open my email? Be wary of spear phishing.

Good news, bad news: The good news is that statistics indicate levels of annoying commercial spam are (*finally*) on the decline. But the bad news is that 2012 has seen rapid increases in the numbers of malicious spear phishing attacks. From the Fortune 500 to your local school district, everyone's a potential target. And recent studies show as much as 65% of global spear phishing attempts occur here in North America. It's getting worse out there.

Being at the forefront of major companies' email security, I've gotten to see firsthand the whole range of spear phishing methods, and the first thing I've noticed is how spear phishing "spoof" emails are getting harder and harder to tell from the real thing. Just the other day, a friend told me she'd received an official-looking email from "Facebook"—that familiar "f" logo, font and the correct shade of blue—saying she'd just been tagged in a friend's posted photo. Not recalling any such recent "Kodak moments" she was anxious to click the link in the email…until she recognized—at the last moment—the link's destination address had nothing to do with Facebook. Would you have done the same?

Many turn-key security products on the market today might only specifically scan incoming email for phony links, but the savviest hackers and cyber robbers are constantly inventing new ways to deceive recipients into giving up their telephone or credit card numbers. They can unleash vicious malware or a simple destructive Excel macro, which can cause you—or your company—costly headaches for weeks. We know the fax machine has long since become an ancient artifact, so think about how dependent we are on email for everything in our professional lives—business communication, purchase transactions, mission-critical contract data. The more ways you rely upon email attachments and links, the more ways spear phishers can exploit any vulnerability.

In Information Week's **10 Security Trends To Watch In 2012**, Alan Brill, senior managing director of the cyber security and information assurance division at Kroll, warned "No one is exempt from (spear phishing) attack." We've already reached the second half of 2012, and every day I hear of more attempts, increasingly sophisticated. Are basic email security products and "mindfulness" alone enough to protect us from every emerging threat? I don't think so.

More than ever, I'm confident that the strongest defense against spear phishing involves employing a matrix of *layered security.* At the heart of any layered approach is a Trusted Sender Recognition solution, augmented by a regular employee education program and staying up-to-date on the latest spear phishing trends. Know your enemy!

You, your co-worker in the next cube, or anyone in your company…it only takes one successful spear phishing attack to potentially wreak havoc upon everything. A savvy, well-secured company knows this…and constantly strides to stay a step ahead.