BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

December 2015 | Briefing 12

DON'T GET STUNG!

SPEAR PHISH ARE DIRECTLY TARGETED AT YOU.

In the Oscar-winning movie "The Sting", Harry Gondorff (played by Paul Newman) explains to his apprentice Johnny Hooker (Robert Redford) that the con that they set up must be so convincing that their mark, Doyle Lonnegan (Robert Shaw) won't even realize that he's been taken.

Today, Gondorff and Hooker might not have needed to use a past-posting scheme to con Lonnegan. Instead they might have used a spear phishing email to bilk him of his money. It would not have made such a fun movie, but it might have been a more effective con.

They might have pored over Lonnegan's presence, including Facebook, LinkedIn, or other online profiles. They will have used Google, or an online service like Spokeo to learn more about his work. They will have built a little chart key relationships – including the victim's family and closest circle of friends (from tagged photos they find online), colleagues (from news articles, social media posts, and Linked-In), managers (from Linked-In and other web sources), and the key players in Lonnegan's professional network (from corporate websites and other online reports). Then they would be ready to spring their trap.

SPEAR PHISH ARE

A Spear Phish is a particularly damaging kind of email attack. Unlike a traditional phishing attack (which is bulk mailed to a large audience of potential victims) **a spear phish is a one-of-a-kind email that has been built specifically to achieve a simple purpose. It is built to attack, beguile, and exploit its intended victim.** It is the product of hours of research by the con artists.

These are especially convincing scams, because it will be clear that the criminals have access to some personal information about the victim. That personal nature of the communication gives the email legitimacy – it is designed to influence the recipient to lower their guard and do something they usually wouldn't do. Unfortunately, spear phish often succeed.

A spear phish is not a bulk email. It is a carefully created email that is literally customized for each target. **The attacking email will appear to come from a colleague, a friend, or a superior.** It will address the victim by name or even nickname, in a familiar context. It may refer to a specific project or work initiative, or something else that gives it legitimacy for the victim. Heed these signs:

THE APPROACH WILL BE FAMILIAR

Spear phishing emails are almost always personal. The greeting will often be familiar, "Eliza" rather "Dear Mrs. Doolittle" or "Dear Eliza". O**ften the email will invoke a familiar name as the sender.** "It's Hugh, Hugh Pickering here." Since the mail is

A SPEAR PHISH - HEED THESE TELLTALE SIGNS:

clearly to you, and appears to be from someone familiar, you are much more likely to engage with the email as a trusted document. The personal touches have given the attack credibility, and lull you into a lower state of vigilance.

IT WILL BE FROM SOMEONE YOU TRUST

A modern criminal will **usually send their spear phish from an email address that closely resembles a familiar email address**. They might misspell the company name, or add a dot to the name that you might overlook. In any event, they will try to make the email look legitimate. In some cases, the criminals have compromised a corporate email account, so that they can actually send their spear phish from a real internal location.

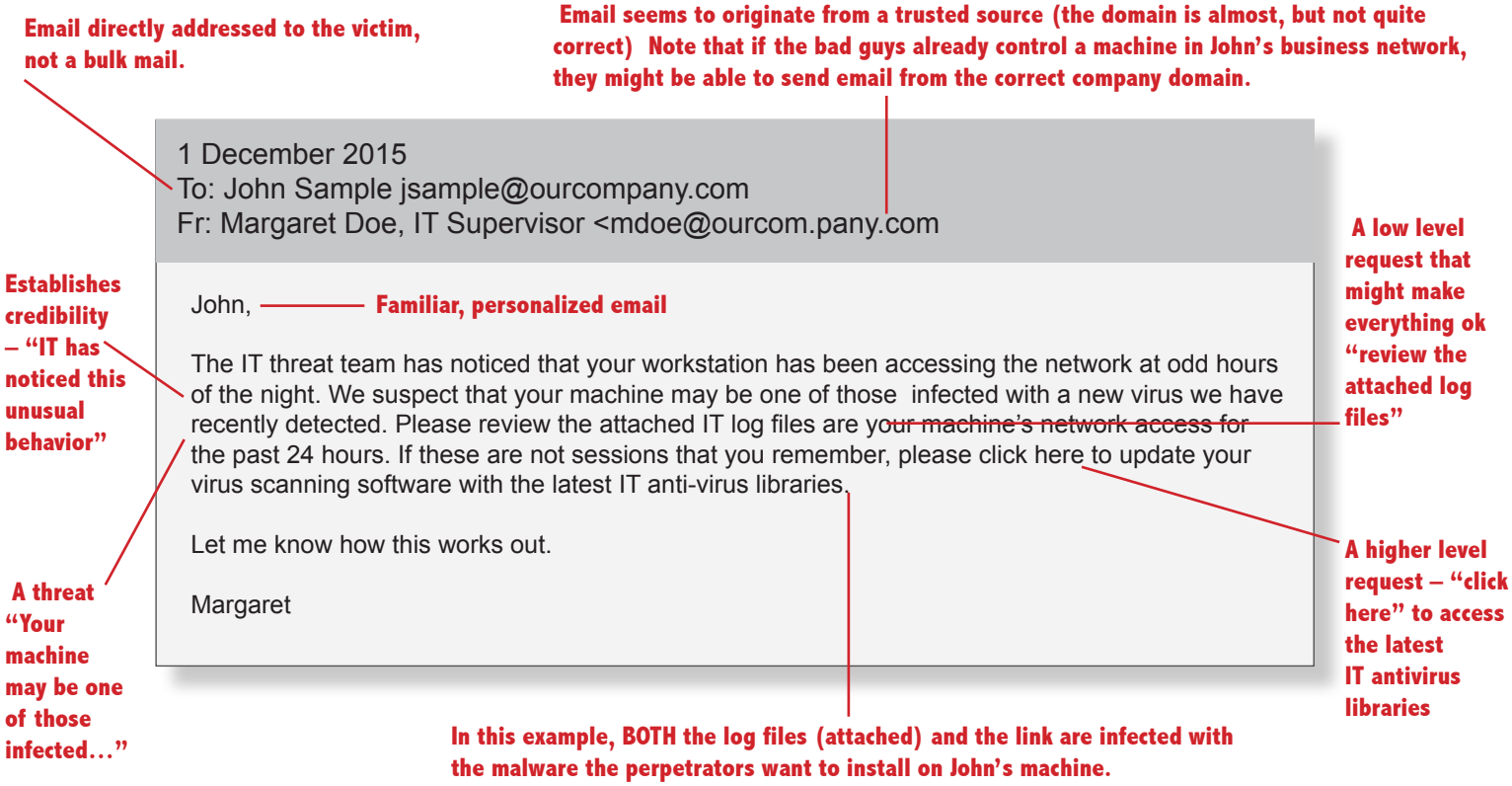
THE EMAIL SEEMS KNOWLEDGABLE

The bad guys will stop at nothing to make their email seem credible. If they can find the information, **they will include a reference to an actual work initiative or project that you (or they) are working on**. This information might have been sourced from public news stories, or from other online postings. "Eliza -- Henry and I have just finished our new "Beginner's Guide to Iberian Meteorology", would you mind giving it a quick read to make sure we haven't left out anything important? Thanks. I'll call you this afternoon to get your feedback. /Hugh.

THE REQUEST WILL SEEM REASONABLE

Often, **the spear phish is designed to prime you to take a small action – to open an attached document, or to click on a link.** A link might take you to a site that automatically downloads malware, or a Trojan onto your machine. The attached file – a spreadsheet, document, graphics file, or PDF, might contain malware that will infect your system. Sometimes the action is more explicit – faxing a confidential report, or even wiring funds to a "partner". Regardless, the spear phisher is leveraging your trust or your eagerness to do a good job, to entice you to cooperate.

ANATOMY OF A SPEAR PHISH EMAIL



USING YOUR TRUST AS A WEAPON

IT IS EASY TO GET FOOLED. TOO EASY.

The spear phishing email will always from someone you know, someone you trust, or someone with authority over you. It may come from a friend outside of work, a colleague, someone you used to work with, or a manager or boss. **It will ask you to do something that you might not normally do, but because of the trust you have in the presumed sender,** or the authority that they have, you do it. And by taking the requested action, you inadvertently provide the criminals with deeper access into your machine, your network, or your organization. In some cases, convincing spear phish have directed employees to transfer funds from company accounts to third party accounts, or convinced employees to email confidential information, even trade secrets to third parties posing as corporate executives.

TAKE FIVE SIMPLE STEPS TO REDUCE YOUR RISK

1. When an email asks you to click on any link, or open any attachment, make sure that you have confidence in the communication.
2. Regardless of how you might feel, before you click on the link or open the attachment, review the email carefully, taking note of the sender, and the sender's domain.
3. Ask yourself, "how likely is it that xxxxxxx would have asked me to do this?

4. At the slightest suspicion, contact the sender via phone or text to validate the message. Do not contact them by replying to the email you received, because it is likely that they will reply and simply say that all is well
5. Make sure your virus scanning and email scanning programs are up to date. An up-to-date scanning program will look for common kinds of malware, or review the security certificates of any web site that you might encounter. That way, IF you click (and you shouldn't) you are more likely to be protected from harm.

Remember – it is far better to be cautious then to run the risk of falling prey to malware, ransomware, or worse. A modern spear phish will seem legitimate. Don't get caught.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.