

A Real Life Spear Phishing Attack



Are you familiar with spear phishing? You should be, because the spear phisher is familiar with *you*! Unlike phishing emails that are usually sent at random from an aggregated list, spear phishing targets specific people. A spear phisher knows your email address, the company you work for and just enough information about you and your position that he or she can use that information to appear to be a friend, a colleague, a boss or even law enforcement!.

What does a spear phishing attack look like? Here's a real life example below. (Actual names and information have been changed.)

At first glance, the email to the right seems legitimate. It addresses the recipient by name. The signature includes a phone number. The body of the email includes Jessica's actual place of employment. **So how would she know this is a scam?**

1 Let's start at the top. Who is Lucas? And why does his email address look so strange? His name isn't in the email address, it doesn't look professional and if it were actually from Lawyers-R-Us PLLC, wouldn't the domain name reflect that?

2 This is the first Jessica is hearing of any sort of testimonial or legal issue. Why would she be subpoenaed out of the blue and via email at that? Wouldn't her supervisors or company lawyers inform her of such things well before she was advised to appear in court?

Wed 4/27/2016 1:18 PM
Lucas Karlsson <wx2@cox.net>
Jessica Martinez • Testimonial Subpeona Letter

To: Martinez, Jessica
1 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

3 Subpeona Jessica Mar... 110KB

Jessica Martinez
Calle Acme Corp 29
33333 Victimville Drive
Spainel, California 99999

RE: CA-6537890

Dear Jessica Martinez,
2

Your case has been set for hearing/trial on 5/6/2016 at 2:00 PM o' clock in the Spainel county courthouse. Your case is before Judge William Kelly in courtroom 175.
You will find it most handy to park on the 019, 022. Judge William Kelly's courtroom is on the second floor.

This is a hearing on Calle Acme Corp Complaint Ref. 1A77654387

We strongly advise you to be present for this. Should you need any further information, feel free to call.

Sincerely yours,

Lawyers-R-Us PLLC
Lucas Karlsson
Tel: 800-999-0966

3 Finally, doesn't it seem strange that there's an attachment when everything she needs to know is written in the body of the email? What is it for?

This very well-crafted spear phishing attack hits all the right notes. If Jessica had let her **fear** take control without studying the email closely, she may have downloaded the attachment and launched it on her work computer, infecting it with malware.

What should you do if you receive an email like this?

At home: delete, delete, delete. At work: follow policy, know how to report any security incidents and, if you're not sure, ask someone immediately!