Don’t Get Harpooned – Avoid Spear Phishing

What is “spear phishing”?

Spear phishing emails are targeted to you and look like they came from a person or organization you trust, but in reality they’re sent by hackers to get you to click on or open something that will give the hackers access to your computer.

Why are you at risk?

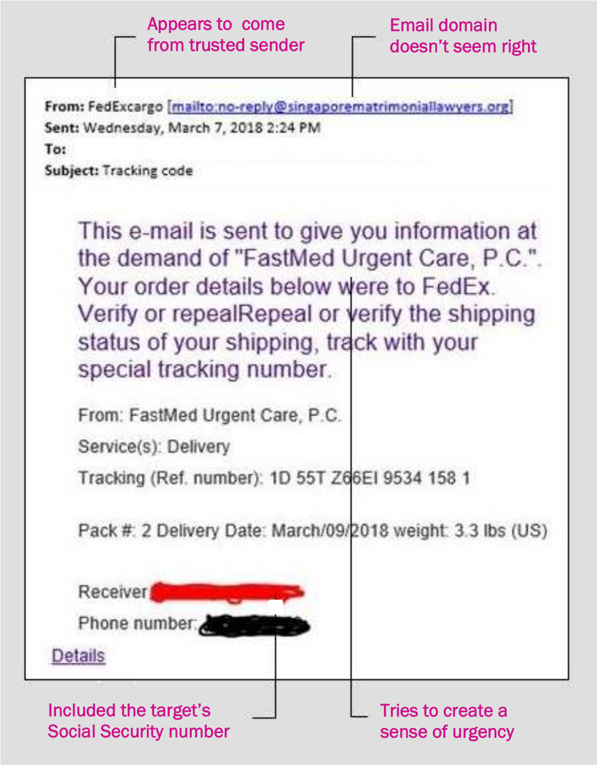
Hackers are actively targeting our organization because we have information that is valuable to them. Specifically, they may be interested in our financial, customer, or employee data. If one employee falls for a phishing attack, our entire system can potentially be accessed.

How to spot a spear phishing email

Hackers have gotten clever in how they design the emails they send out to make them look legitimate. But spear phishing emails often have the following characteristics:

- Made to look like they come from someone you’d trust:
  - FedEx, a bank, or some other outside organization you would recognize
  - Departments within our own organization, such as HR or IT
- Try to create a sense of urgency about responding
- May contain your personal information to encourage you to trust the email
- Direct you to click on a link to take action
- Ask you for your username and password, sometimes by replying to the email, but more often by clicking on a link that takes you to a site where you’re asked to input the information. **IMPORTANT: Nobody at our organization will ever ask you for your password.**
- Contain email addresses that don’t match between the header and the body, are misspelled (like *@gmaill.com*), or have unusual formats (*@company-othersite.com*)
- Have links or e-mail addresses that show a different destination if you hover over them

Here is an example of a recent phishing email:



Appears to come from trusted sender

Email domain doesn’t seem right

From: FedExcargo [mailto:no-reply@singaporematrimoniallawyers.org]
Sent: Wednesday, March 7, 2018 2:24 PM
To:
Subject: Tracking code

This e-mail is sent to give you information at the demand of "FastMed Urgent Care, P.C.". Your order details below were to FedEx. Verify or repealRepeal or verify the shipping status of your shipping, track with your special tracking number.

From: FastMed Urgent Care, P.C.

Service(s): Delivery

Tracking (Ref. number): 1D 55T Z66EI 9534 158 1

Pack #: 2 Delivery Date: March/09/2018 weight: 3.3 lbs (US)

Receiver [redacted]

Phone number: [redacted]

Details

Included the target’s Social Security number

Tries to create a sense of urgency

What you should do if you get a suspicious email

If you suspect that an email is a phishing email:

- Do not open any links or attachments in the email
- Notify our IT department
- **If you’ve already opened a link or attachment, disconnect your computer from the internet but do not turn it off, and then immediately call IT**