Spear Phishing *in Action*

Unlike traditional phishing scams that are usually sent at random from an aggregated list, spear phishing targets specific people. In this attack, the scammer researches the target to gather as much information as possible, such as place of work, job title, and any personal details available to the public. They then use this information to gain and abuse the victim's trust, sometimes posing as a co-worker, friend, or even law enforcement.

To the right is an example of what a spear phishing email might look like. At first glance, the email seems legitimate. It addresses the recipient by name. The signature includes a phone number. How would Jordan know this is a scam?

1. ***Who is Robert? In the email he claims to be part of IT, but Jordan knows that IT at his company uses the email IT@company.com.***

2. ***Normally, system updates are done remotely. Why would Robert need Jordan to download and install something manually?***

3. ***This sense of urgency represents a classic red flag that the email is a phishing attack. The scammer wants Jordan to feel pressured into taking immediate action.***

What should you do if you receive an email like this? Use extreme caution when handling requests to download attachments, click on links, or divulge sensitive information. Report all suspicious emails to the appropriate parties immediately. And always follow organizational policies.

Monday 11/15/2020 9:42 AM
From: Robert MacMahn <tech@company.com>
To: Oswin, Jordan
Subject: Jordan Oswin - System Update required

Hey Jordan,

This is Robert from IT. We are pushing out new security software and I need you to download the attachment and run it on your workstation immediately.

Thanks,
Robert MacMahn
IT Desk
(234) 326-4634

sec-update-786.zip