Phishing

Welcome back. In this video, we're going to take a look at some examples of phishing. As you probably already know, phishing is a type of social engineering. Effectively, the attacker tries to get the target to disclose information about their login credentials.

They can also be looking for information such as bank details, or they could be trying to get the end user to download some form of malware. The attack comprises of the attacker coming up with an email which includes some form of link, which the user is invited to click on. At this point, the user could be taken to what looks like a legitimate website to provide their login credentials too.

And that information is then being sent to the attacker. Alternatively, it could be some form of drive-by download, where the end user clicks on a link, and it downloads malware. Or even an attachment could be downloaded also. We're going to start by taking a look at specific examples. At each example, you're asked to pause the video and consider whether you think they are an example of phishing. And if so, why or why no? Let's start with this example. This example is a genuine email. Despite the fact that it has a number of different links to click on, and there is a lack of identifying information, with the exception of a three digit partial bank account number, it is indeed genuine. If we look at the full details, the Received From domain matches the From domain, which is shown in the email overview.

Moving now on to the second example, this is an example of phishing. First off, this is not a company that I've ever purchased from before. Second of all, it is sent in French, which is not my primary language, and certainly not a language that I claim to speak very well at all.

You'll also notice that some of the language is a little bit strange. If you have a look at what the links are at the top, we have Wife, Man, Child, House, and Good Plans, which is a little bit strange. You'll also notice that there are some links there, and it's asking you to click on that link, which is also a little bit dubious. But let's look at the full details of the original message within the email client. You can do this in all email clients.

In particular, for example, with Gmail, if you open a message, then look at your dropdown

options, and say Show Original. If we look at the metadata at the top, we can see from the Received, it's from something called lemustdesdeals.com, not Bon Prix, as you would expect to see if it was authentic. You can spoof From part in the message view.

This can be relatively easy to do. All you need is an SMTP server, which is the protocol for e-mail, and the right sort of mailing software. You can then fill in the From part of the email. It may or may not get through. It depends on the receiving email server.

Because SMTP, Simple Mail Transfer Protocol, allows any computer to send an email claiming to be from a source domain or address, those performing phishing attacks could they change the From part of address to look like it comes from an official domain. As a result of this, we had to find a solution.

The sender policy framework, or SPF, provides a way for mail servers to verify that the IP address sending the email was indeed authorised to send email on behalf of the domain--

so the domain being something like apple.com or google.com. The mail server receiving the email needs to compare the IP of the origin in the message with the IP listed and the SPF record for the email address' host. So for example, under Google, there will be a list of IP address ranges which have been identified by Google.

The receiving email server can then check the IP against this list. If the IP doesn't match, it can be identified as spam and not originating from Google itself. Note that this is a somewhat simplified overview of this. There's clearly a little bit more to it. If you are interested, there's plenty of information out there to have a read through.

But one thing to notice here is that it is the responsibility of the receiving email server. And as you might imagine, not all email servers do this, which is why I said it depends on the email server which is receiving it as to whether it will actually let through the email or not. Let's have a look at another example.

As you might expect, this one is indeed a phishing email. There is no identifying information. It's asking the end user to login as soon as possible. It provides a link which doesn't go to Apple, which you can see if you were to hover over it. It simply doesn't even look official. And we could see these issues backed up by the full detail of the message, where the domain in the Received From is not the same as the domain in the From field further down.

And even looking at that From field, it's fairly apparent it's not an Apple domain. What we have shown here is an example of spear phishing. Spear phishing is where the attacker is targeting you specifically. It's not just spam, the same email sent two lots of different addresses, using something like a botnet. They tend to know a little bit about you specifically, and the email can be personalised with other information. The example shown here shows

that somebody is trying to look for a job, and you've got a URL which is somewhat obfuscated, due to the use of tinyURL. Spear phishing is definitely a bit harder to detect.

So it relies on your own vigilance. Upon clicking on some of the links within a phishing email, you may be downloading malware or perhaps going to a phishing website. These websites look very much like the legitimate websites. But the data is obviously going to the attackers. So if you provide credentials, that information is being communicated to the attackers, who can then go to the legitimate website and access your account. Hopefully you managed to get most of those right.

But as you'll notice from the examples, some of these are not necessarily terribly easy to detect. And indeed, some legitimate emails can be misunderstood as phishing emails, because of how they are structured. Some of the techniques used in phishing, as an example of social engineering, includes the typical social engineering behaviours--

leveraging authority, impersonation, pressure and solution, and pretext. Why not see if you can identify any of these elements in examples which you might get through your work or through your own personal email? There are, of course, other ways of trying to mitigate phishing emails coming into your organisation or your personal email. If you're working within an organisation and you are somehow responsible for this kind of thing, then you might also want to look at raising stuff-awareness in training. There are penetration testers who perform social engineering testing. They can send phishing emails to your department employees and see whether they actually follow through.

If they do follow through, then they can be followed up with, in order to train them not to do so in the future. Well, that's it for this video. I hope you've enjoyed it, and I'll see you next time.