Phishing Email Requesting Direct Response

This form of attack involves receiving a phishing email that purports to be from the bank.

The most common example is that the email sets out that the bank has updated their system and that, as a result, the recipient is required to update their bank account details or they would be unable to access their accounts after a certain date. The email requests the recipient to follow a link to carry out this task. Clicking on the link brings the recipient to a website that appears very similar to the authentic website of the bank.

By updating the bank account details on this fraudulent website, the individual provides the fraudster with their login details to the online banking, thus facilitating a fraudulent withdrawal from their accounts.

It should be noted that when the email is viewed in the mail inbox of the email service the name of the bank appears in the “From” field; however, when the email is opened the address of the sender in the “From” field is normally completely different.

Precautions Specific to this Type of Attack

Ensure your anti-virus software is fully up-to-date and set to automatically update.

Financial institutions will never send you an email asking you to provide any of your personal banking details.

Always check the authenticity of the senders address in the “From” field after opening the email.