deycom
OUR TEAM SUPPORTS YOUR TEAM

How to Avoid a Phishing Attack

Introduction

Even with a robust email filtering system in place, there is always a chance that a rogue email could slip through to your email inbox. That is why it is crucial for all computer users to understand the potential risks. It is essential to be aware that you may come across deceptive emails aimed at coercing you into making fraudulent payments or divulging sensitive information.

This type of cyber threat is known as 'Phishing,' and to help everyone to know what to look out for, we have created a comprehensive guide to help you to spot these threats and take proactive steps to reduce the risk of falling victim.

For a deeper dive into email security, don't hesitate to reach out to Deycom at 059 9130777 or via email at info@deycom.com. We are here to help you safeguard your organisation.

What is a Phishing Attack

A Phishing attack is when a scammer sends an email that is designed to trick the recipient into believing the email is from a legitimate person or company. Scammers will use a technique called Spoofing that can make the email look like it is has come from a trusted source or they may hack a legitimate email account and use this account for fraudulent purposes.

This makes it extremely important to verify that emails are legitimate before replying to them especially if you are being pressured into doing something urgently or something that involves a financial transaction.

How to identify a Phishing Email

While Phishing emails are designed to trick the recipient into thinking they have received a genuine email, very often there are aspects of the email that don't look right. Here are some issues to look out for:

- Many phishing scams have poor spelling, grammar and / or punctuation. The email may also include logos and graphics that might not be what you would expect from a large organisation.
- The email might not contain your name, and instead it might be addressed to a 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Phishing Emails will often put you under pressure to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'I need your help ASAP', or click here 'immediately'.
- It is quite common to be told that the sender of the email cannot be called on their phone, they are in an 'urgent meeting' or at 'all-day conference'. This is to persuade you not to ring the legitimate contact.
- Scammers will sometimes use the name of a senior individual within an organisation to carry out a phishing attack. This is to exert pressure on the individual who gets the email because they feel obliged to respond quickly. So be very careful of any unusual emails that appear to be from senior personnel.
- A lot of Phishing emails relate to parcel deliveries issues, unauthorised payments on a credit card, or issues around email accounts. They are all designed to get the recipient to react quickly without thinking.

Advanced Phishing Attacks

More advanced phishing attacks, known as spear phishing are also a threat. These are more targeted and will often contain less obvious indicators and the sender will appear to know information about the target person and the company they work for.

Scammer may also hack a legitimate email account and then use this account to send out phishing emails. Again, these are very difficult to detect and while it appears the emails are coming from someone you know they may in fact be from a hacked email account. These types of attacks are normally used for financial fraud. The sender will for example try to trick the email recipient into paying a legitimate invoice to a bogus bank account, and this is called Invoice Redirect Fraud.

Scammer may also pretend to be a senior individual within the same organisation in an attempt to trick individuals to make a payment from their personal bank account or on their own debit card, saying that the company will reimburse them afterwards. This is why it is important that all computer users are aware of the risks.

How to reduce the risk

Scrutinize: When dealing with business related emails always ensure the name and email address look correct and that the grammar and logos look normal. Be very wary if anything looks unusual.

Double Check: If you have any concerns about an email you receive, especially concerning financial requests, please call the sender of the email. Remember very often scammer will say they are not available on the phone as part of the scam.

Suspicious Email Address: Be very wary if you receive an email from someone you know but it is from an unfamiliar address especially if it is from a non-business account, such as Gmail or Yahoo.

Updating Details: Whenever you are asked to update a supplier bank details by email always verify the request by phone and make sure you are calling the correct number, not a phone number in the email.

Website Links: Be very careful when clicking on links or opening attachments in emails especially if you are being asked to provide sensitive information.

Ask for Help: If you feel you have been the victim of a Phishing attack or you have clicked on an unusual email link reach out for help from your IT support team. It's better to check it out than ignoring it.

Key Phishing Attack Tip

It extremely important to verify that emails are legitimate before replying to them especially if you are being pressured into doing something urgently or something that involves a financial transaction. If you have concerns, call the person who sent you the email to verify their request is legitimate.

Next Steps.

We hope you have found this guide useful and if you require any further assistance with email security or cyber security within your organisation, please contact our sales team and we would be delighted to help.

Contact Us

info@deycom.com
www.deycom.ie

Carlow: 059 9130777
Kilkenny: 0567813060
Kildare: 045397118
Dublin: 012233844