deycom

OUR TEAM **SUPPORTS** YOUR TEAM

How to Avoid a Phishing Attack

Introduction

Even with a strong email filtering system, there's always a chance that a rogue email might slip through into your inbox. That's why it's crucial for everyone to understand the risks. You may encounter emails designed to trick you into making fraudulent payments or revealing sensitive information. This type of cyber threat is called 'Phishing'. To help you spot these threats and reduce the risk of becoming a victim, we've created this simple guide.

If you need more detailed information on email security, feel free to contact Deycom at 059 9130777 or via email at info@deycom.com. We're here to help you safeguard your organisation.

What is a Phishing Attack

A Phishing attack occurs when a scammer sends an email designed to trick the recipient into believing it's from a legitimate person or company. Scammers often use a technique called "spoofing," which makes the email appear as if it's coming from a trusted source. Sometimes, they might even hack into a real email account and use it to carry out fraud.

It's essential to verify that emails are genuine before replying, especially if you're being pressured to act quickly or if the email involves a financial transaction.

How to identify a Phishing Email

Phishing emails are designed to deceive you, but there are often clues that something isn't right. Here’s what to look out for:

- **Poor Spelling, Grammar, and Punctuation:** Many phishing emails have obvious mistakes. They might also include logos and graphics that don't look quite right.

- **Generic Greetings:** If the email doesn't contain your name and instead uses terms like 'valued customer,' 'friend,' or 'colleague,' this could be a sign that the sender doesn't know you and that the email is part of a scam.

- **Urgent Requests:** Phishing emails often urge you to act quickly. Be suspicious of phrases like "send these details within 24 hours" or "I need your help ASAP.“

- **Unreachable Senders:** It's common for phishing emails to claim that the sender can't be contacted by phone because they're in a meeting or at a conference. This is to stop you from verifying the request.

- **Impersonating Senior Staff:** Scammers sometimes use the name of a senior person within your organisation to pressure you into responding quickly. Be cautious of any unusual emails that appear to come from someone senior.

- **Common Scams:** Phishing emails often involve parcel delivery issues, unauthorised payments, or email account problems. These are designed to make you react without thinking.

Advanced Phishing Attacks

More sophisticated phishing attacks, known as spear phishing, are also a threat. These are more targeted and can be harder to spot, as the sender often appears to know details about you and your company.

Scammers may hack into a real email account and use it to send phishing emails. These emails can be particularly tricky to detect and are often used for financial fraud. For instance, the scammer might try to trick you into paying a genuine invoice to a fake bank account—this is known as Invoice Redirect Fraud.

Scammers might also impersonate a senior person within your organisation, asking you to make a payment from your personal bank account or debit card, claiming the company will reimburse you later. This is why it's vital to be aware of the risks.

How to reduce the risk

Scrutinise Emails: Always check that the sender's name and email address look correct. Be wary if anything seems off, such as unusual grammar or unfamiliar logos.

Double Check Requests: If you have any doubts about an email, especially one that involves money, call the sender to verify it. Remember, scammers often claim they're unavailable by phone.

Suspicious Email Address: Be cautious if you receive an email from someone you know but the email address is unfamiliar, especially if it's from a non-business account like Gmail or Yahoo.

Verify Bank Details Changes: If you're asked to update a supplier's bank details via email, always verify the request by phone using a known number, not one provided in the email.

Be Careful with Links and Attachments: Be extra cautious when clicking on links or opening attachments in emails, especially if you're being asked to provide sensitive information.

Seek Help Immediately: If you think you've been the victim of a phishing attack or clicked on a suspicious link, contact your IT support team right away. It's better to be safe than sorry.

Key Phishing Attack Tip

Always verify that emails are legitimate before responding, particularly if they involve an urgent request or a financial transaction. If in doubt, call the sender to confirm the email is genuine.

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

Disclaimer:

The information provided in this phishing guide is intended for informational purposes only. While we have made every effort to ensure the accuracy and reliability of the content, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.
This guide is not a substitute for professional advice, and we strongly recommend that you consult with qualified experts and professionals in the field of disaster recovery for specific guidance tailored to your unique circumstances.

In no event will Deycom Computer Services or its employees be liable for any loss or damage, including but not limited to, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of this guide.

By using this guide, you agree that you do so at your own risk, Deycom Computer Services shall not be held responsible for any consequences resulting from the use or misuse of the information provided herein.