unitec
Accessible Expertise

PHISHING

What it is, and how to protect your business

What is phishing? Phishing is the act of fraudulently obtaining sensitive information (such as usernames, passwords or credit card information) or fraudulently instigating a financial transaction by impersonating a legitimate entity.

How are phishing attacks carried out? They can be carried out in a variety of ways - via emails, fake websites or by phone call, are often are very convincing and include elements of social engineering.

What are the dangers to an organisation? Businesses can suffer financial losses, data breaches and damage to their reputation due to successful phishing attacks.

Some examples of phishing attacks.

- A company “director” requesting a large financial transaction.
- A “supplier” notifying a payables department of a change to banking information prior to a large scheduled transfer.
- A “bank” asking you to click on a link to log-in immediately fix some problem with an account. In this example, the link brings the user to a fake page (one that looks almost identical to the original). If the user enters their details here, the criminals have the key to their accounts and can initiate transfers.

Cybercriminals can be quite sophisticated - in some cases, they monitor company emails for weeks, and so can strike at the perfect moment, like just before a scheduled payment to a vendor is due to be processed.

How can you protect your organisation from falling victim to phishing attacks? Education is the best defence. Phishing is an ongoing threat, and the risk is even larger for staff working in the financial areas of your business.

We’ve compiled some useful tips and listed them on the next page. Be sure to share them with your staff - the more educated everyone in your organisation is regarding this type of crime, the less likely it is you’ll find your organisation falling victim.

If you’d like to review any of these items with your Unitec Account Manager, or discover other ways to protect your organisation from cyber threats, please get in touch.

GET IN TOUCH

sales@unitec.ie
www.unitec.ie
0818 222 132

Education is your best defence against phishing

Follow these tips to minimise the risk of your organisation becoming a victim of a phishing attack.

Watch out for **generic greetings**

Many phishing campaigns are carried out in bulk, meaning the cybercriminals will use greetings similar to “Dear Sir/Madam” or “Dear Customer” rather than your name. If your name isn’t listed, be immediately suspicious. However, having your name listed is not a guarantee of legitimacy.

Examine the **sender information**

Carefully examine the sender information, particularly the email address. Sophisticated phishing attacks will make a subtle change to a legitimate email address in the hopes it won’t be noticed by the receiver. For example, it might be a little difficult to notice the discrepancy in and address like info@bankofiireland.com (did you see the double “i” the first time?).

Examine **links** before clicking

If an email asks you to click on a link, ensure that you ensure it’s pointing exactly where you expect. Hover over the link to view the actual destination. If it’s different to the link text, don’t click. You can always access the legitimate website by typing the usual address into your browser’s address bar and going from there.

Be wary of **urgency**

It’s in the criminals’ best interest to have you act as soon as possible. Often phishing emails will try to create a sense of urgency in the hopes that the receiver will react without taking the precautions we’re mentioning here. An email from your “bank” might inform you that your accounts will be seized if you don’t log in within the hour, for example.

Pick up the **phone**

Have procedures in place for when certain changes are requested. The staff member processing these changes can easily verify the legitimacy of a request by simply picking up the phone for confirmation. It’s one quick, simple way you can protect your organisation from becoming a victim.