Phishing awareness from ramsac

ramsac
at the heart of IT

Phishing emails are becoming more sophisticated and harder for a user to spot, resulting in an increase in successful cybersecurity breaches. The key to protecting your data is ensuring that your staff know how to spot a fraudulent email and how to keep your business safe. That is why we offer a testing and awareness subscription from just £75 per month, to increase cybersecurity awareness and to train your "human firewall".

What are phishing emails?

A phishing email is an email that attempts to scam a user into sharing information, or that invites a user to click on a link that may contain a virus. They are often designed and written in a way that looks like an official email that appears to come from a trusted contact. They have quickly become one of the most prevalent forms of cyber attack.

The testing and awareness subscription

From just £75 a month, we will carry out random simulated phishing attacks, ensuring that every user receives a very realistic phishing email at least twice a year. The emails mimic real phishing emails and if the user clicks on a link they will be taken to a safe web page, that highlights what they have just clicked on and offers them an immediate online training session on how to spot attacks in the future.

Phishing is on the rise

Spotting a phishing email is an important skill to master because phishing accounts for 90% of data breaches. And once hit, 15% of people successfully phished will be targeted at least once more in the same year.

The frequency of phishing attacks is on the increase with a 40.9% uplift in successful attacks last year.

Knowledge is power

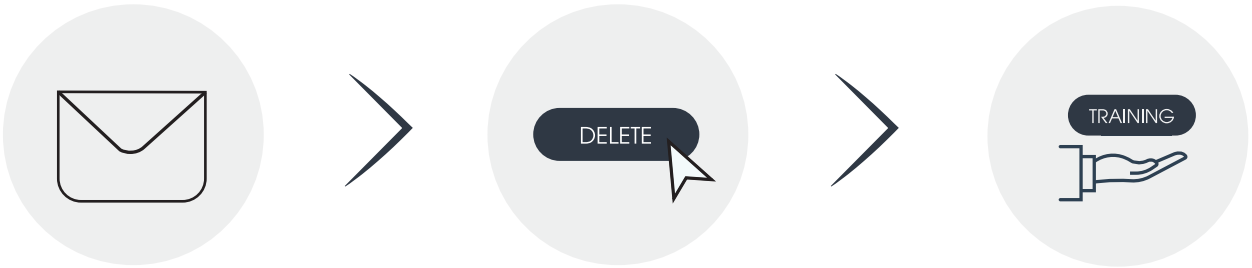
ramsac
at the heart of IT

Every 6 months the management team or a nominated person in your organisation will receive a detailed report on who has clicked and who has not clicked on our test emails and of those that have, how many of them have then gone to complete the online learning.

This extra knowledge will help you improve your cybersecurity by identifying any weaknesses in your human firewall and where additional training may be needed.

6 ways to spot a phishing email

1. Check the "from"address - is it different from usual, are there subtle spelling errors or is the user using a Hotmail or Gmail account?
2. Be suspicious of untidy design.
3. Look out for spelling mistakes.
4. If it's too good to be true, it probably is.
5. Consider context - were you expecting this email?
6. Always question any email that is asking you to make a payment, even if it appears to be from someone you know.



EMAIL IN | *DELETE OR CLICK* | *IF CLICKED - ADDITIONAL TRAINING*

For more information on our **phishing awareness subscription** or for help protecting your organisation against cybercrime please call us on **01483 412040,** email **info@ramsac.com** or visit our website **www.ramsac.com.**

ramsac
at the heart of IT