What is a Phishing Attack?

Phishing is the fraudulent practice of sending emails purporting to be someone else to extract personal information, passwords and credit card numbers from the recipient and eliciting fear and urgency.

Phishing is extremely common, is on the rise, and is getting more sophisticated. According to Intel, 97% of email users around the world are unable to identify a sophisticated phishing email, therefore your employees are your business' weakest link.

What are the Costs of a Phishing Attack?

A successful Phishing attack can significantly impact a business. In 2015, the average total cost for a data breach was $2.82M. Financial services businesses are more likely to suffer data breaches.

Reputational cost to a brand arguably does more damage. It can take years to build trust and relationships with your clients. Many businesses never recover from this.

Research by Deloitte has found that a third of consumers would take their business to a competitor following a breach.

No solution will provide 100% security from these scams. The key is to ensure that your staff are well-educated and able to detect such attacks.

If you think your business is safe because it has not yet happened to you, **please think again**. Make sure your staff are aware of the following ways to identify Phishing emails.

How to Identify Phishing Emails

1. **Is the sender who they say they are?**
    - Check the email address of the sender. If it looks suspicious, delete it.
    - A legitimate business name in the URL doesn't mean it is legitimate.

2. **Spelling and grammar mistakes can be a dead giveaway.**
    - Does the sender typically converse in this manner? If not, delete the email.

3. **Is the email asking for personal or payment information?**
    - Triple-check the sender is who they say they are. Make a call to the sender if you're being asked to transfer money.
    - Most businesses do not ask you for your personal information via email. Don't give them up!
    - Legitimate businesses will never ask you for login/sign-in information.
    - Fake invoices are the number 1 type of Phishing lure.
      Source: Symantec 2017 Internet Security Threat Report

4. **Does it feel right? Is it threatening?**
    - Pay attention – if it doesn't feel right, it's probably not right.
    - Be wary of emails threatening action, or requesting urgent action.

Keeping Your Business Safe

To complement your staff's increased awareness, the following solutions should never be optional.

- **Invest in a reputable email security suite**
    - Stop most Phishing Attacks before they hit a staff's Inbox. Remember, your staff are your business' weakest link.
- **Invest in Password Manager software**
    - A password management solution automatically logs in or autofills a login page, taking away the risk of a staff member keying in sensitive information into a spoofed (faked version) of a website.
- **Invest in the correct gateway security appliances**
    - This can stop access to spoofed login pages and websites.

Contact IPO Digital Solutions for more information on how we can help stop these Phishing attacks in your business.