EMAIL PHISHING AND PROTECTING YOUR BUSINESS

Email Phishing is largely becoming the most utilized tool for scam artists, and they are becoming more and more creative in their approaches, copying logos, using URL's that are similar to well-known brands, hoping to find any individual that will open and respond to their emails with no further delay.

Email Phishing Scams are a simple means of accessing your private information, and in-turn using your private information to exploit funds from bank accounts and credit cards.

Examples of Phishing Scams in recent times have been from: Banks, Credit Unions, Electricity, Gas, Telecommunications Companies, and software companies.

How to Identify Email Phishing, or emails that seem suspicious?

- Check the email address has been sent from the registered domain name of a company, EG: Email from East Bank displays an email of: admin@hotmail or gmail.com instead of admin@eastbank.com.au

- Requests for personal details, and bank or credit card details. A legitimate company you are dealing with will not request the above information from you, unless you have specifically made an enquiry to that accord.

- Investigate the information they have presented to you, as in most cases the scammers make a calculated guesses as to your personal information as they don't have it Investigate what the Email is advising and if it is even relevant to you. As an example receiving an email from East Bank, and you bank with Bank North, calculated guesses being made by scammers.

- Check any email suggesting that you must upgrade your details, as there has been a security breach, maintenance or upgrade, as this is usually a ploy to have the recipient divulge their personal details.

In short, should you believe any email is a potential risk:

- Do not open it, and do not click on any attachments it may contain, simply delete the email.

- Never outline any personal information , including bank details or credit card details unless you are sure it is a trusted company

- Report any to the authorities using the below link.

If you have any further enquiries , please review the attached ACMA link that provides a comprehensive review on Email Phishing .

https://www.scamwatch.gov.au/protect-yourself/attempts-to-gain-your-personal-information