PHISHING AWARENESS

WHAT IS PHISHING?

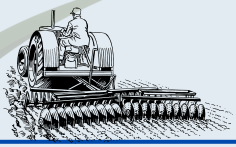
Phishing is a type of scam where hackers trick you into giving them your personal information, such as passwords and banking details. They often do this by pretending to be a trusted entity.

KEY SIGNS OF PHISHING

- Scammers often create a false sense of urgency to make you act quickly.
- Check the sender's email address closely for signs of spelling mistakes. Government departments such as the Department of Primary Industries rarely make spelling mistakes.
- Be cautious of links that don't match the official website.
- Be wary of requests for information that the sender doesn't usually ask for.
- Scammers might send emails from addresses that look legitimate but are slightly altered. For example, they may swap the letter o for the number 0.

HOW TO PROTECT YOURSELF

- Verify the source by contacting the sender via alternative means, such as phone.
- Look for spelling and grammar mistakes. Pay attention to odd measurements or currencies.
- Be sceptical of emails with too good to be true offers.
- Anti-virus software can help protect your devices if you accidentally fall victim to a phishing scam. Think of it as having a backup generator to keep your dairy or irrigator operational during a power outage.



PHISHING AWARENESS

PHISHING VIA CALLS AND SMS

- Use the Google Messages app on your mobile phone to block phishing SMS and calls.
- Use 1831 (landline) or #31# (mobile) before a number to keep your phone number private.
- Don't engage with callers claiming to be from trusted brands, especially if they ask for personal information.
- If someone asks you to pay using gift cards, it's a scam. Legitimate businesses and government departments will not demand payment via gift cards.
- Don't answer calls from private numbers unless you are expecting a call.

HANDLING EMAIL ATTACHMENTS

- Always scan attachments with antivirus software before opening them.
- Avoid opening files with extensions like .exe, .bat or .zip as they can contain harmful code.
- If you receive a Microsoft Office file, disable macros t prevent malicious code from running.
- Regular updates to your operating systems and devices will help protect you against new threats.

ADDITIONAL RESOURCES

Scamwatch

Scam Awareness

Agriculture.gov.au

Frut Growers Vic

AgForce

Farm Weekly