Scam Awareness

Scams are designed to trick people into handing over money, personal information, passwords, or sensitive content. Criminals often pretend to be trusted organisations, government agencies, banks, service providers, employers, friends, or romantic partners. Modern scams are increasingly sophisticated and may combine emails, phone calls, text messages, fake websites, and even AI-generated voices to appear legitimate.

Impact of Scams

Being scammed can have far-reaching consequences that extend well beyond financial loss. The impacts can include stress, anxiety, embarrassment, and a loss of confidence, as well as identity theft, compromised accounts, damage to your credit rating, loss of privacy, time-consuming recovery efforts, strained relationships, and an increased risk of being targeted by future scams.

Common Types of Scams

Phishing Scams

Email or SMS messages pretending to be from legitimate organisations that encourage you to click a link, open an attachment, or provide login details.

Imposter Scams

Criminals posing as banks, government departments, utility providers, employers, or technical support staff to obtain money or personal information.

Romance Scams

Scammers create fake online profiles, build trust and emotional connections, then request money for emergencies, travel, or investment opportunities.

Gift Card Scams

Victims are asked to purchase gift cards and provide the card numbers or PINs. Legitimate organisations do not accept gift cards as payment.

Spiritual or Curse-Removal Scams

Scammers claim a person is cursed or spiritually afflicted and demand payment for rituals or cleansing services. Some use recordings of private interactions for blackmail.

Blackmail and Sextortion

Criminals obtain private images, videos, or personal information and threaten to release them unless money is paid.

Warning Signs

- Urgent requests for money or action
- Unexpected prizes, lottery wins, refunds, or financial offers
- Requests for passwords, PINs, or verification codes
- Requests to pay using gift cards, cryptocurrency, or wire transfers
- Refusal to meet in person or video call
- Suspicious email addresses, links, or websites

Protect Yourself

- Stop and think before responding.
- Check email addresses, links, and website URLs carefully.
- Contact organisations directly using official contact details you find independently.
- Never share passwords or verification codes.
- Never pay with gift cards.
- Enable multi-factor authentication (MFA) on important accounts.
- Be cautious about sharing personal, financial, or intimate information online.
- Never send money to someone you have only met online.

Remember

Scammers rely on urgency, fear, trust, loneliness, and excitement to stop people from thinking clearly. Your best defence is to slow down, verify information independently, and never rush into making payments or sharing personal information.

Remember: If something sounds too good to be true, it probably is.

If you think something might be a scam, or you're simply not sure, don't hesitate to contact one of our Peer Navigators for advice, clarification, and support. Positive Life NSW also offers a one-on-one **Digital Mentors Program**, where you can build your digital confidence, learn how to identify scams, and develop practical skills to stay safe online.