什么是 phishing scam (网络钓鱼诈骗)?

phishing scam（网络钓鱼诈骗）正在盛行。

phishing（网络钓鱼）是指诈骗者冒充他人，例如您信得过的人或公司。

但为什么称之为 phishing scam（网络钓鱼诈骗）呢?

就像用诱饵钓鱼一样，诈骗者会引诱您上钩，以便获取您的个人信息。

冒充我们的 phishing scam 诈骗者可能会声称您有资格获得退款，或者您的帐户有问题，并提供一个指向冒牌网站的链接。

他们的一个惯用伎俩是制作一个假的 myGov 登录网站。

诈骗者通过复制我们的名称、标识和颜色，让这些虚假的 myGov 网站看起来很逼真，因此很难发现不同之处。

如果您点击该链接并提供您的信息（例如您的 myGov 登录信息），诈骗者可以使用您的信息来登录您实际的 myGov 帐户并访问您的绑定服务。

然后他们就可能以您的名义索取政府付款或窃取您应得的款项。

这被称为盗窃身份。

更多信息请访问 **servicesaustralia.gov.au/scams**

What is a phishing scam?

There are a lot of phishing scams around.

Phishing is when a scammer pretends to be someone they're not, like a trusted person or company.

But why are they called phishing scams?

Just like using bait to catch a fish, scammers lure you in so they can catch your personal information.

Phishing scams that pretend to be us might say you're eligible for a refund or there's a problem with your account with a link to a fake website.

One trick they like to use is to make a fake myGov sign in website.

Scammers make these fake myGov websites look real by copying our name, logo and colours, so it can be hard to spot the difference.

If you click on the link and provide your information like your myGov sign in details, the scammer can use your details to sign into your real myGovaccount and access your linked services.

Then they can claim government payments in your name or steal payments you were meant to get.

This is called identity theft.

For more information go to **servicesaustralia.gov.au/scams**