

If it sounds too good to be true it probably is!

How to avoid being scammed

1. What are scams?

Scams are fraudulent schemes operated by dishonest people to steal money or something else of value such as personal details or data.

2. Types of scams

There are many types of scams, many of which are now perpetrated through the Internet or social media. The DFSA's website has information on typical scams including:

- cold calling
- fake bank emails/phishing
- Ponzi schemes
- lottery scams
- boiler room scams
- advance fee frauds

3. What to look out for

Here are a few indicators of a scam:

- unexpected contact e.g. a call or an email out of the blue
- companies using generic email accounts (e.g. Gmail)
- if what is offered sounds too good to be true (e.g. inflated returns on investments, easy access to loans, surprising inheritance benefits or unexpected competition wins or "guaranteed" ways to make fast money or a high-paying job for little effort), then it usually is
- if any person asks you for personal details, account numbers, login codes or passwords
- being pushed into making a decision on the spot

4. How to avoid being scammed

You can avoid being scammed by:

- checking for the company on the relevant regulatory agency's website
- carrying out Google searches. The DFSA and other regulators regularly issue Alerts on particular scams
- never giving out personal information and particularly bank accounts numbers, login codes or passwords
- not making advanced payments until you are sure of the legitimacy of the company
- make sure all of your accounts have a strong password
- make sure any websites you use are secure
- use safe and secure WiFi connections

- keep operating system and virus protection software up-to-date
- avoid unexpected contact such as phone calls, letters and emails

5. What to do if you are the victim of a scam may include:

- stop sending money immediately
- contact your financial institution if you have sent money or shared your banking details
- report the scam to local authorities
- be vigilant for follow-up scams
- warn friends and family about scams and any relevant business association or other contacts you know
- change online passwords
- engage with authorities if you suspect you are the subject of identity theft
- contact your local consumer protection agency

For more information go to <http://www.dfsa.ae/Your-Resources/dfs-a-alerts#How-to-avoid-being-scammed>.

1. **Disclaimer:** *The information set out above is not all encompassing and is not any form of, and must not be relied upon on any basis whatsoever as, legal or other advice, but rather is for general informational purposes only.*