Protect yourself from becoming a victim of fraud

In the past years, there has been an increase in scammers impersonating trusted organizations like Partners Group. Such criminals carefully prepare their scams to trick you into letting your guard down and sharing personal information or making payments.

Protect yourself from scams:

- Stay alert when you are contacted by a person you do not know, be that via telephone, email, social media or otherwise.
- Take a moment to question and research if the request or offer you have received could be fake.
- When in doubt, individually research a company's official telephone number instead of calling a number given to you by a potential scammer.
- If you believe that you have fallen for a scam, immediately contact your local law enforcement as well as your bank to report what happened. Local law enforcement and your bank will support and advise you on any further steps to take.

Please note that Partners Group:

- does not provide financial services or directly market products to retail clients
- does not ask for any kind of payments without you having signed proper paperwork
- does not accept any payments without having conducted all legally and regulatory required client due diligence and anti-money laundering checks including verification of investor identity and origin of money
- does not have a cryptocurrency division and will not offer you the possibility to invest in cryptocurrency
- will not ask you to make an investment via telephone, a non-official business email address or a social media account
- will allow you to always verify any officially issued payment requests by using Partners Group's Document Verification Service (https://verify.partnersgroup.com/)
- is in no way affiliated with AG Partners, AGPartners Group, Partners Japan Co. or the domain agpartners-group.

While Partners Group does post links to job openings on social media (LinkedIn and Instagram), we do not extend job offers via our social media accounts.

Potential fraud case which has been recently reported to Partners Group:

- Cryptocurrency investment scam

A person using different aliases, messaging services via professional and employment oriented online platforms (e.g. LinkedIn) or a generic email domain (e.g. gmail.com) is presenting him-/herself as an employee working for Partners Group (or a company with a similar name) and offering randomly identified individuals the possibility to make an investment into cryptocurrency. He/she gives the victims a telephone number to call to verify his/her identity, and has in certain instances also requested permission to take remote control over the victim's personal computer.

To prevent becoming the victim of such a scam, please only call Partners Group's official telephone numbers or official email contacts to verify such requests before making payments of any kind or giving any of your personal information. Partners Group's official telephone numbers are available here and our official email addresses are available here.

How to stay safe online

Only visit trustworthy websites

A secure website will start with https:// in front of the address. Never enter confidential data if you are uncertain about the legitimacy of a site.

Use of trusted computer

When accessing confidential online information, make sure you use a trusted computer or mobile device. Do not use public computers such as computers in internet cafés, lobbies, etc. to access online services or perform financial transactions.

Log off the online session and clear the browser cache after every session

It is recommended to manually log-off all online sessions once finished and to clear the cache data. The browser’s cache stores the contents of all the web pages that have been visited. Hence it is advised to clear the cache to safeguard private information and prevent another user from viewing what you have entered.

Content encryption

Partners Group advises clients to consider the use of encryption technology to protect highly sensitive or confidential information.

Keep your software up to date and disable unneeded services

To be even better protected, update operating systems, anti-virus and firewall products with security patches or newer versions on a regular basis. Consider the use of spam filters and even "antiphishing" software to help screen out potential phishers on websites and emails.

Generally, disable unnecessary services such as printer or file sharing when accessing the internet in order to avoid infection by malware.

Backups

Regular backups of critical data are essential and Partners Group advises clients to regularly take backups of such data.

Phishing

How to spot suspicious calls and emails and the best way to address them

Phishing is an attempt to access sensitive information such as passwords, bank details and account information through seemingly legitimate telephone calls, websites and emails.

Based on advice by financial services regulators such as the Monetary Authority of Singapore (MAS), Partners Group educates clients and staff on the dangers of email-based phishing. The information herein mainly focuses on the My Partners Group portal.

Always review unsolicited contact

Clients should be attentive to any unexpected email, phone call or fax that claims to be from an asset manager, bank, credit card or online company. Never share confidential information with anyone if in doubt about the sender or the reason for the request. If any doubt about a communication received from Partners Group arises, please contact your client relationship manager and delete such junk or chain emails.

Don't click on links or download attachments from suspicious emails. Moreover, don't install software or run programs of unknown origin.

Sometimes it can be difficult to differentiate a phishing email from a genuine one. Beware of unusual sender addresses, spelling mistakes and strange elements such as the tone of the email, disclaimers and logos. If there is any doubt about the authenticity of an email, please contact your client relationship manager.

Verify payment requests

When receiving bank details over email, we recommend to call the recipient on a known documented number that is not in the email to verify the details.

Ignore emails about allegedly unusual account activity

Phishing emails often aim to incite curiosity or a sense of urgency in order to get the recipient to click a link or open an attachment. Genuine organizations are highly unlikely to contact clients by email in order to inform them about suspicious payments or transfers from their account.