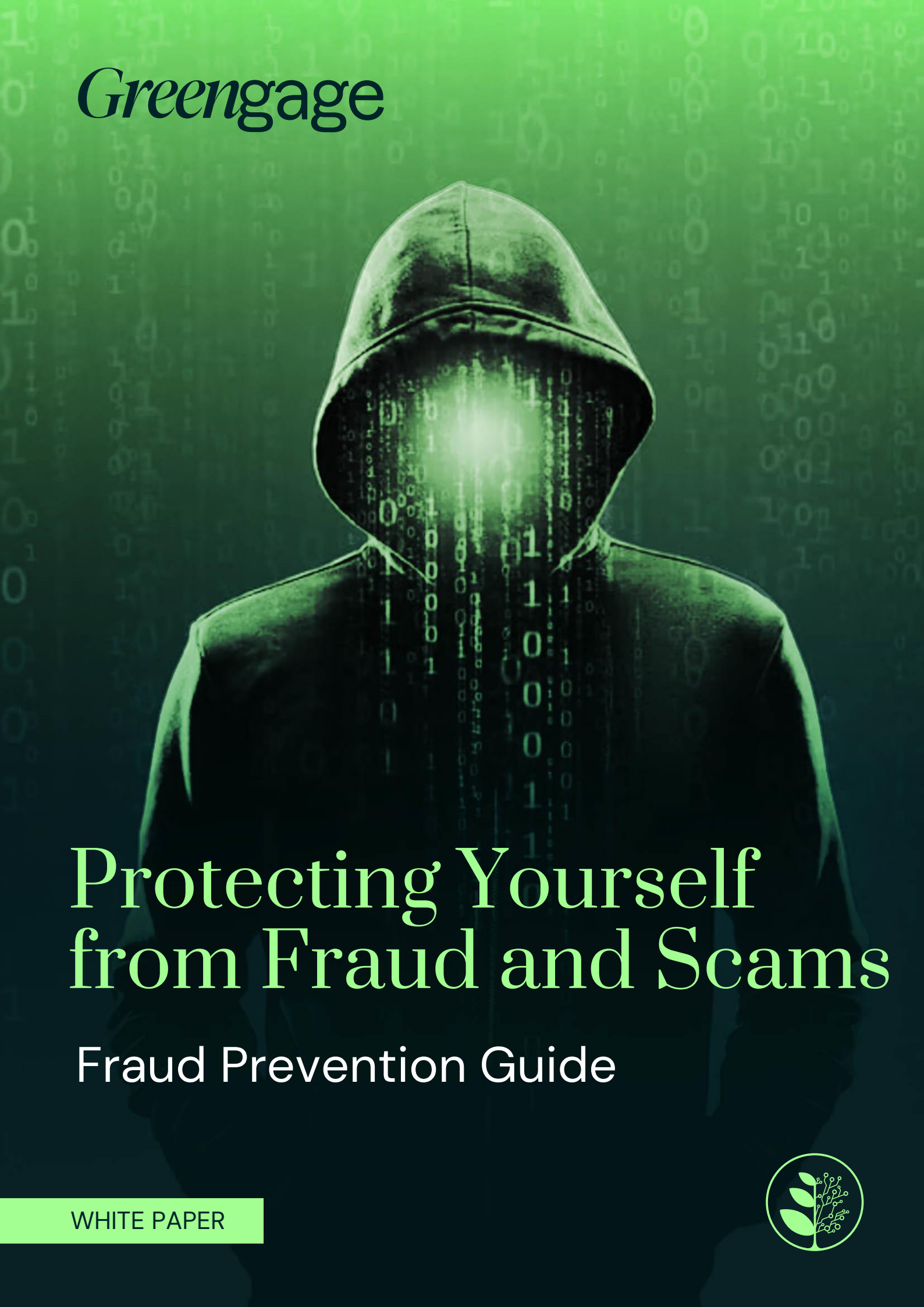
Greengage



Protecting Yourself from Fraud and Scams

Fraud Prevention Guide

WHITE PAPER

Introduction

Greengage aims to empower our clients with the tools and awareness needed to prevent fraud, while also prioritizing their protection. We understand this will come from a balance between our commitment to protecting you to the best of our capabilities and providing the tools and awareness you may need to avoid it happening to you.

Fraudsters can make their scams tricky to detect, especially if you are not aware of their methods. Being a victim of fraud can be devastating experience, causing mental distress and financial loss for individuals and businesses. Staying vigilant and well informed allows you to protect your most important data like passwords, account details and personal details from being compromised.

Greengage strives to promote a culture founded on fraud prevention, awareness, accountability, and the detection of actions that are considered to be suspicious.

Please remember that Greengage will never ask you:

1. **For any of your passwords, PINs[1] or OTPs[2]**
2. **To withdraw, deposit or transfer any money to prove your identity, especially within a time limit**
3. **To download any application via a link other than the official App Store or Android Store links provided on the official Greengage website.**
4. **Call and randomly ask for any of the following details:**
   - Your full name
   - Your date of birth
   - Your telephone number
   - Your email address
   - Your home town or any personal questions

If you receive any suspicious calls, please hang up immediately and call us at **0208 610 4444**, or if you receive any email, you can forward it to **info@greengage.co.**

1 PIN – personal identification number
2 OTP – one time password

Red Flags to Look out for

- **Messages that just don't look right** – be on the lookout for typos or bad grammar, or email headings that sound confusing, almost as if on purpose.
- **Someone you trust contacts you with a strange request** – scammers may pretend to be someone you know, and have an inexplicably urgent request that is out of their character.
- **If something sounds too good to be true, it probably is** – scammers may entice you with a prize of a lifetime or an investment opportunity with low risk but high rewards.
- **Odd payment requests that are out of the ordinary course of business** – Be aware if someone or an organisation you know quite well is asking for a fee upfront, especially via an unusual payment method.

Types of Scams

Phishing – Avoid Taking the Bait

Phishing scams involve a fraudster contacting you, whether it be via email, the telephone or text messages, to gain your trust and encourage you to share sensitive personal information, click on fake links that contain malware or make payments to an account to "prove" your identity by creating a false sense of urgency. The most common types of phishing scams include:

- **Smishing** – uses common messaging apps or text messages to target individuals. Phone numbers that these messages come from are often in an irregular format.
- **Vishing** – uses phone calls to contact victims, often impersonating reputable organisations.
- **Spear Phishing** – a targeted and personalised attack on a specific victim.
- **Whaling** – generally aimed at high profile individuals.
- **Angler Phishing** – uses social media to target victims using fake corporate accounts

Always be careful when approached by strange requests like this, and if you are unsure about the caller's identity, remember you can always call them using a phone number you know is genuine to check.

One Time Password (OTP) Scams

When you log into most secure websites to carry out an action now, they may ask you to provide a one time password (OTP) sent to your mobile phone via text or email. Fraudsters attempt to get around this requirement by getting in touch with you and pretending to be a service provider, asking for your OTP under some pretence. Unless you have requested the OTP yourself and you are sure about the reason it has been generated, never share your OTP over a phone call, text or email with anyone. Remember, you would never be asked for an OTP randomly by your provider or any reliable company.

Money Transfer Fraud

Scammers have been calling customers claiming to be from the fraud team of the financial organisation they have accounts with and advising the customer that their account has been compromised, and their money must be moved urgently into a "safe" account. This is actually an account that the scammer controls, from where it becomes quite challenging to retrieve stolen funds. Remember, you always have the option to hang up and call your provider yourself if you feel even the slightest bit unsure, as it is better to carefully consider your decisions than to make any rash choices or be pressured by an unknown caller.

Card Fraud

When your card is stolen, not only can your card be used by the thief to make unauthorised payments, your details are also at high risk of being sold onwards to other criminals for further illegal activities. Signs you have been a victim of card fraud could be that your card has been rejected when you try to make a payment, or you find transactions on your statements that you don't remember making.

Crypto Scams

Phishing scams branch into the crypto world as well, with fraudsters aiming to gain access to your holdings through scamming their way to your crypto keys. As almost all phishing scams go, you could be encouraged to click a link to a fake website where scammers can steal your account details. Scammers may also try to entice you with a once-in-a-lifetime opportunity which is apparently low-risk but high reward, where you just need to transfer a small fee as investment. Realistically, you would possibly never see that crypto ever again as it will be sent to the scammer's account, so avoid making any rash decisions without thinking it through.

How Can you Protect Yourself?

Do's

- Keep important documents secure and ensure they are not accessible to anyone other than you or someone you trust
- Keep your log in details for your accounts and important accounts stored safely, and never share them with any third parties you do not know.
- If you feel pressured to take action immediately over the phone or email, be on your guard. You can always hang up and call the service provider yourself to verify identity independently.
- Always take your time before responding to any text or email. Being hasty can risk overlooking clear signs of a scam.

Don'ts

- Avoid visiting your online account services through unfamiliar links. Only access your accounts through the official website or your mobile app.
- If you are connected to a public Wi-Fi network, try to avoid accessing internet account services until you can connect to a safe and secure network.
- Avoid using easy to guess or simple passwords.
- Avoid oversharing information on social media, especially if it can reveal sensitive information or allow someone to easily impersonate you.

Remember to TAKE FIVE and:

- **STOP** – Taking a moment to stop and think before parting with your money or your information could keep you safe.
- **CHALLENGE** – Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush you or panic you.
- **PROTECT** – Contact your provider immediately if you think you've fallen for a scam and report it to Action Fraud on 0300 123 2040. If you are in Scotland, please report to Police Scotland directly by calling 101 or Advice Direct Scotland on 0808 164 6000.

Remember, organisations such as HMRC do not send notifications regarding tax refunds, fines or penalties, or request any personal or financial information over emails, text messages or phone calls. If you receive any suspicious communications claiming to be from HMRC, you can forward any emails to phishing@hmrc.gov.uk or text messages to 60599.

STOP
CHALLENGE
PROTECT

TAKE FIVE TO STOP FRAUD™

Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

https://www.takefive-stopfraud.org.uk/

Greengage

For more info:

info@greengage.co

Painters' Hall,
9 Little Trinity Lane,
London EC4V 2AD UK

www.greengage.co