Swallowfield Safe & Secure

A plain English guide to protecting your money, identit and peace of mind — online, by phone, and at your front door

Disclaimer: *This guide is provided by Swallowfield Parish Council for educational and community awareness purposes only. It does not constitute legal or financial advice. Fraud tactics evolve rapidly, and while all information is provided in good faith to assist residents, the Parish Council and its Councillors accept no liability for any financial loss or damage arising from reliance on this material. Always verify urgent requests directly with your bank or Thames Valley Police, and consult professional advisors for personal financial security.*

What we will cover

- The **most common and most damaging** scams currently hitting UK residents
- How to **spot the red flags** (online, phone, and doorstep)
- Simple **prevention habits** that stop most scams
- **Your rights** if money is lost (bank transfer scams / APP fraud)
- **Who to contact** – the fastest routes to help and reporting

Top Scams

Top scams to watch for (1/2)

- **Parcel delivery ‘smishing’ (fake RM/Evri/DPD texts)**
  - **Red flag**: ‘small fee’ + link to re-deliver / reschedule
- **Bank, HMRC or police impersonation calls**
  - **Red flag**: urgency + instruction to move money to a ‘safe account’
- **‘Hi Mum / Hi Dad’ WhatsApp messages**
  - **Red flag**: new number + urgent bill + request for transfer

Top scams to watch for (2/2)

- **AI voice cloning and deepfakes**
  - **Red flag**: a loved one ‘in trouble’ + demand for immediate money
- **Fake parking fines & ‘quishing’ (QR code scams)**
  - **Red flag**: sticker QR codes; texts about PCNs with payment links
- **Investment / ‘get rich quick’ scams**
  - **Red flag**: guaranteed returns, crypto hype, celebrity endorsement videos

Quishing Example

- **Fake parking fines & ‘quishing’ (QR code scams)**
  - **Red flag**: sticker QR codes; texts about PCNs with payment links

They are fast, free and easy to create by anyone, and there has been a significant rise in their use to defraud.

Whenever there is doubt, there is no doubt. Don’t trust the link or image – go direct to the app or website.

How scammers win

- **The Impersonator**: bank, police, HMRC, council, NHS
- **The Digital Trickster**: links in texts/emails, fake QR codes
- **The Doorstep Deceiver**: rogue traders & pressure sales
- **The False Friend**: romance and long-con scams

Key point: scams change their story, but not their method. How old is the Nigerian Prince correspondence scam?

What to do and what NOT to do

Prevention: the critical DOs

DO take	**DO** take a breath and pause – scammers rush you
DO talk	**DO** talk to someone you trust before you act
DO heed	**DO** heed bank warnings (e.g., Confirmation of Payee name mismatch)
DO use	**DO** use long passphrases (three random words)
DO hang up & call back	**DO** hang up and call back using a trusted number (or 159 for banks)

SWALLOWFIELD PARISH COUNCIL

Prevention: the critical DON'Ts

DON'T click	**DON'T** click links in unexpected texts/emails – type the website yourself
DON'T share	**DON'T** share PINs, passwords, or one-time codes
DON'T allow	**DON'T** allow anyone remote access to your computer
DON'T trust	**DON'T** trust caller ID – numbers can be spoofed
DON'T be	**DON'T** be embarrassed – professionals trick smart people every day

If you think you've been scammed: first 30 minutes

- **Stop contact with the scammer and keep evidence** (texts, numbers, screenshots)
- **Call your bank immediately** (use 159, or the number on your card)
- If you clicked a link: **change passwords** (starting with email), enable 2-step verification (2FA or MFA)
- **Report**: scam texts to 7726; scam emails to report@phishing.gov.uk
- **Report** the crime to Report Fraud / Action Fraud (online or 0300 123 2040)
- If someone is at your door and **you feel unsafe: call 999**

Your rights and who to call

Fridge card: 3 steps that stop most scams

1. **STOP: Pause. Don't click. Don't transfer money**
2. **CHECK: Talk to someone. Use a trusted number (or 159 for banks).**
3. **ACT: If you've lost money, call your bank immediately and report it.**

Report it:

Texts	→	7726
Emails	→	report@phishing.gov.uk
Fraud	→	0300 123 2040

Who to contact (quick list)

- **Your bank**: dial 159 (then say your bank)
- **Report scam texts**: forward to 7726
- **Report phishing emails/websites**: forward to report@phishing.gov.uk
- **Report fraud/cybercrime**: Report Fraud (formerly Action Fraud) – 0300 123 2040
- **Citizens Advice consumer helpline**: 0808 223 1133
- **Victim Support** (emotional support, 24/7): 0808 16 89 111

Your rights: the safety net

- APP fraud reimbursement became mandatory for Faster Payments/CHAPS from 7 Oct 2024
- In most cases, eligible victims must be reimbursed – cap is £85,000 per claim
- Banks can refuse only in limited cases (e.g., proven ‘gross negligence’)
- **Important:** the gross-negligence exception does not apply to vulnerable consumers
- If you disagree with a decision, you can escalate to the Financial Ombudsman Service

Keep the newsletter information handy and share it

Electronic copy available

SAFE & SECURE IDENTIFYING AND AVOIDING SCAMS

A community friendly guide to help residents spot, stop, and report the scams currently causing the most harm in the UK.

THINGS TO WATCH OUT FOR

- **Parcel delivery texts (smishing):** messages claiming a courier needs a small fee to redeliver a parcel. Don't click the link — go to the courier's official website.
- **Bank or police impersonation calls:** callers may claim your account is under attack and ask you to move money to a "safe account." Banks and police will never ask you to transfer money.
- **"Hi Mum / Hi Dad" WhatsApp scams:** a new number claims to be a family member and asks for urgent money. Always call the family member on a number you already have.
- **AI voice cloning / deepfakes:** scammers can now imitate voices. If a loved one sounds odd, hang up and call them back on a trusted number.
- **Fake parking QR codes ("quishing"):** stickers over real QR codes can send you to a fake payment page. Pay via the official council parking app or by cash/card if you are unsure.
- **Investment and romance scams:** if it sounds too good to be true or someone asks for money for an emotional emergency, be suspicious.

SIMPLE RULES TO FOLLOW

- **Pause.** Scammers rush you. Stop and think.
- **Check with someone you trust.** A second opinion helps.
- **Call back using trusted routes.** Don't stay on the line; use numbers from your bank card or official website.
- **Never share PINs, passwords or one time codes.**
- **Don't allow remote access** to your computer.

STOP / CHECK / ACT

- **STOP:** Don't click; don't transfer.
- **CHECK:** Call a trusted contact or the organisation using a number you already have.
- **ACT:** If money sent, **call 159;** forward **texts to 7726;** report email to **report@phishing.gov.uk**

SWALLOWFIELD PARISH COUNCIL

Supporting & additional info

SWALLOWFIELD PARISH COUNCIL

Sources (official)

- PSR: APP fraud reimbursement protections (start date 7 Oct 2024; cap £85,000)
- GOV.UK / NCSC: report@phishing.gov.uk and guidance on reporting phishing
- Ofcom: 7726 reporting for scam texts and calls
- Stop Scams UK: 159 hotline
- City of London Police: Report Fraud service (replaces Action Fraud; number unchanged)
- Victim Support: 24/7 Supportline

What the latest UK data is flagging (2025–26)

Fraud is increasingly digital and industrialised, with AI speeding up convincing impersonations.

Identity fraud and account takeover (ATO) remain major drivers of harm (often via stolen personal data and SIM swaps).

High-harm scam themes continue to include courier/courier-style scams, investment fraud and romance fraud.

Doorstep scams (local ‘rogue trader’ pressure)

- Uninvited traders offer ‘urgent’ repairs (roof tiles, driveways, gardening)
  - **Tactic:** start work quickly, then demand hundreds of pounds — often by bank transfer
- **Golden rule:** never agree to work from someone who knocks uninvited
  - Use recommended/vetted local tradespeople; get written quotes
- If you feel threatened or they refuse to leave: call 999

Romance scams: the ‘false friend’

- A **scammer builds trust** over weeks/months via social media or dating sites
  - Then asks for money for emergencies, travel, medical costs, or ‘fees’
- **Red flags**: secrecy, isolation, moving chat off-platform, repeated crises
- **Rule:** never send money or share financial details with someone you haven’t met

Fake officials (HMRC / NHS / Police / Council)

- Calls or texts claim you owe a fine, have an unpaid bill, or are due a refund
  - **Tactic:** urgency + threat of court action + link to pay now
- **Rule:** don’t use the link — find the official website/number yourself
- If unsure: talk it over with someone you trust before paying

Further Reading

Below are more examples of scams and how scammers succeed. It is recommended you familiarise yourself with good practices by seeking the latest advice and information.

Wherever there is doubt, there is no doubt.

- **Sharing Password, Codes & Secrets: do not share these**. They are your responsibility in the same way as your banking PIN.
- **Public/unsecure Wi-Fi**: **do not trust unsecured connections**. Use a secure Wi-Fi and/or VPN (virtual private network) if on an unsecured connection (your mobile network **is** secure).
- **Mobile Phone Lock Screen**: **do not allow your message content to be readable** on your lock screen. Account Takeover (ATO) Fraud is often facilitated through this.
- **Scannable Codes & Links** (including QR Codes): **do not trust they are genuine**. Go to the official app or website.
- **Phone Numbers**: **do not trust that the number you see is the person calling** – numbers can be faked. Always hang-up and call back using the organisation's official phone numbers.
- **Calling Back**: **do not call a potential scammer back**. If genuine, an organisation will try again, or through other means. Also commonly know as the Wangiri (one-ring) scam, designed to get you to call back (often to a premium line).
- **Voice & Image Deep-Fake**: **do not trust that the voice you hear is the one you know**.
- **Mobile Voicemail**: these can be a way in for scammers to set '*call forwarding*' to act as you when you bank contact you (for ATO). If you have a voicemail, ensure that you have **updated the security information** from first set-up (**or turn off voicemail**).
- **Account Takeover (ACO) Fraud**: Usually to intercept secure codes to take over your financial accounts.
- **Multi-factor Authentication**: Where possible, set-up *2-Factor Authentication* (2FA) or *Multi-Factor Authentication* (MFA), as these provide better security. Or, use your device biometrics and 'passkey' set-ups for app where supported.
- **Passwords vs Pass-Phases**: Password are often easy to break (aka 'brute force' attacks). Instead, try using memorable phases which are personal to you.

Disclaimers & Notices

Best Intentions & Context: This program is created and distributed in good faith, strictly as educational guidance to help protect the residents of Swallowfield and surrounding Parish Council areas.

Not Professional Advice: The information provided in this guide is for educational and general community awareness purposes only. It does not constitute formal legal, financial, or professional security advice. Residents should always consult their bank, financial advisor, or legal representative regarding their personal circumstances.

Limitation of Liability: While every effort has been made to ensure the accuracy of this information at the time of publication, Swallowfield Parish Council and its Councillors accept no liability for any financial loss, damage, or distress resulting from the use of, or reliance upon, the information contained in this presentation/leaflet.

External Services: This guide contains contact details and references to third-party organizations (such as Action Fraud, the Financial Ombudsman Service, and various banks). The Parish Council does not control these entities, is not responsible for their services or response times, and does not formally endorse any commercial products.

Evolving Threats: Cybercrime and scam tactics evolve rapidly. The methods described here are based on current known trends, but criminals constantly adapt. Always remain vigilant and prioritize your personal safety.