Cyber Fraud Alert from Police Scotland

Smishing is a type of phishing attack where mobile phone users receive text messages containing a Web site hyperlink, which, if clicked would download a dangerous internet virus to the mobile phone.

- If a text message has a link to a webpage – DELETE IT!!
- Text Alerts about unusual transactions – DELETE IT!!!

Phishing is when criminals use fake e-mails or web links to obtain sensitive information about people, such as passwords, usernames, or bank account details.

- E-mail uses generic terms like 'Dear account holder'.
- E-mail is threatening and states that urgent action is required.
- E-mail contains an unrecognisable link.
- Spelling errors in the e-mail.
- E-mail address is different from trusted company's website.
- Unexpected e-mails from a company you have no business with.
- No padlock sign on website and no https:// at the beginning of web address.

Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business and fools the victim into thinking he or she will profit.

- NEVER give out any personal or financial information over the phone, including your PIN, passwords or online codes, as a genuine bank will NEVER ask you for this.
- If in any doubt HANG UP and call your bank directly

Doorstep Crime and Bogus Callers

How can I protect myself from doorstep crime?

Remember, it's your home. There's no reason why anyone should ever enter your home against your wishes.

- Be on guard if someone turns up unexpectedly. If you're not sure, don't answer the door.
- Keep front and back doors locked and if you're not sure, don't answer the door.
- Only let callers in if they have an appointment and you have confirmed they are genuine.
- DPHA contractors will normally get in touch with you to make an appointment prior to their visit and will always carry identification. However, if you are in any doubt, contact our Customer Services Team on **0141 435 6533** to confirm an appointment
- Always ask for identification badges of anyone you answer the door to, but don't rely on them. Identity cards can be faked – if you are not expecting the visit, phone the company to verify their identity.
- Some companies offer a password system. Ask your utility providers if this can be used and if you have a password with a company make sure the caller uses it.
- Never let people try to persuade you to let them into your home even if they are asking for help – they may not be genuine.
- If someone is persistent, ask them to call at another time and arrange for a friend or family member to be with you.
- Never agree to pay for goods or give money to strangers who arrive at your door.
- Don't keep large amounts of money in your home.

Further information can be obtained on Police Scotland website at **www.scotland.police.uk**