PLEASE DO NOT REPLY TO THIS MESSAGE.

If you or someone you know is vulnerable and has been a victim of fraud, please call Essex Police on 101.
Report fraud or attempted fraud by contacting Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

SIM-SWAP FRAUD – HOW CRIMINALS HIJACK YOUR NUMBER TO ACCESS YOUR ACCOUNTS

An unusual one this week, but a fraud that has increased by 400% since 2015!

Sim-swap fraud is where a criminal tricks your network into transferring your mobile number to a Sim card in their possession meaning they receive all calls and texts intended for you – including any one-time security passcodes required to access your accounts.

How do they do it?

There are a number of ways criminals obtain your data – either through social media, paying for stolen data or through social engineering (fake emails, texts or phone calls that trick you into giving out your details).

With this information they then pose as you in order to contact your network provider and request that your number is switched to a new Sim card that they have. They will then get your number swapped so that they can receive all of your calls and text messages.

'Tell2, protect many' is a communication initiative that empowers you to spread crime prevention messages to others in your life, who otherwise may never know.
Start with 'tell2' and ask them to do the same. It starts with YOU!

What can I do to protect myself?

1. **Protect your mobile account**
   Add a password or passcode to your mobile account

2. **Clean up your online profile**
   Restrict who can see your social media profiles which can often contain information that is then used in security questions (i.e. name of first school, date of birth, children's names etc)

3. **Beware phishing attempts**
   Remember to be vigilant if you get calls, texts or emails asking for information. Remember ABC – Never Assume they are genuine, Never Believe they are genuine and Always Confirm they are genuine before giving out personal details.

4. **Recognise the signs**
   Call your provider immediately if you receive unexpected texts or emails about 'porting your Sim' or a PAC request, or if you suddenly lose phone signal.

5. **Inform your banks**
   If your Sim has been swapped, alert your banks immediately in case the fraudster tried to make a transfer from your account.

6. **Use 2FA apps**
   Remove your phone number from any websites or accounts that use it to reset passwords. There are other apps that use the physical device to authenticate requests, rather than the phone number.

In the current climate, mobile phones are a vital lifeline for many people. Please ensure you tell your family and friends about how to protect their number from criminals!

For more information on Sim-swapping and personal stories about how people have been affected please read this Which? news article.