Be Fraud Smart!
essex.police.uk/befraudsmart
ESSEX POLICE
Protecting and serving Essex

Essex Police Fraud Alert System

8

17th September 2020

UK FINANCE

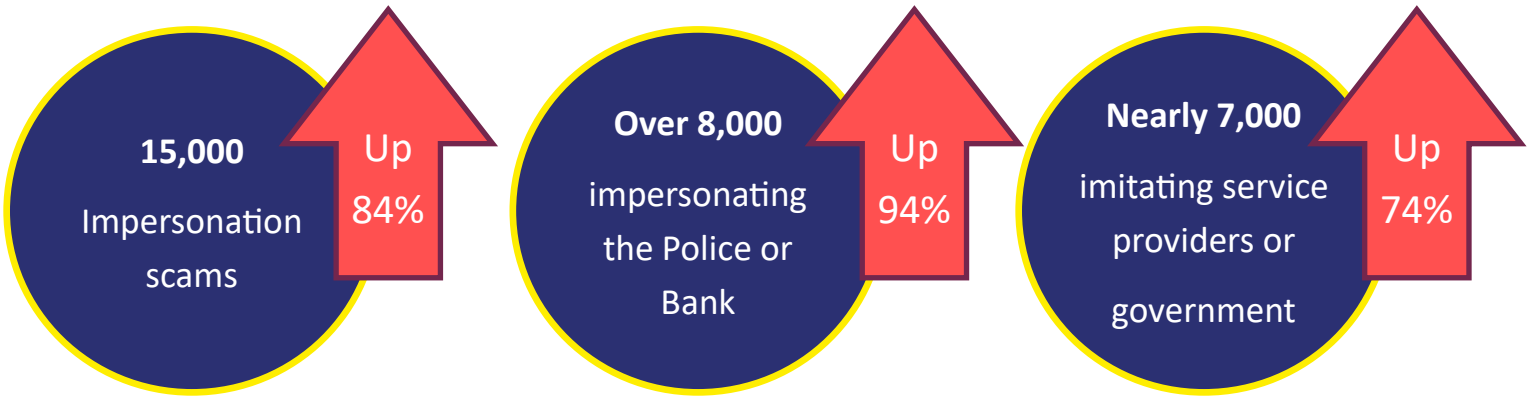
IMPERSONATION SCAMS ALMOST DOUBLE IN FIRST HALF OF 2020 AS CRIMINALS EXPLOIT COVID-19 TO TARGET VICTIMS

- Almost 15,000 impersonation scam cases reported in the first half of 2020, up 84 per cent compared to the same period last year
- £58 million lost to impersonation scams in January to June 2020, up three per cent on the previous year
- Public urged to beware of criminals exploiting Covid-19 to impersonate the police, banks, or government organisations

UK Finance is urging people to be aware of criminals exploiting Covid-19 to target their victims, after figures revealed a sharp rise in impersonation scams in the first half of this year.

Impersonation scams occur when the victim is convinced to make a payment to a criminal claiming to be from a trusted organisation. This could include the police, a bank, a utility company, or a government department.

JANUARY—JUNE 2020



£58 million lost

Keep up to date with fraud and do *even more* Online at essex.police.uk

CALL ESSEX POLICE 101
IN AN EMERGENCY ALWAYS CALL 999

Essex Police Fraud Alert System

Scams involving the criminal impersonating a bank or the police often begin with a phone call or text message claiming there has been fraud on the victim's account. The customer is then convinced that to protect their money they must transfer it to a 'safe account' which actually belongs to the fraudster. Other common scams involve text messages or emails claiming a victim must settle a fine, pay overdue tax or return a refund that was given by mistake.

Covid-19 related impersonation scams include:

- Criminals claiming to be from an airline or travel agency, offering refunds for cancelled flights or holidays
- Criminals exploiting the growing numbers of people working remotely, by posing as IT departments or software providers and claiming that payments are needed to fix problems with people's internet connection or asking for remote access to the victim's computer.

Criminals will tend to research their targets first, using information gathered from other scams, social media and data breaches in order to make their approach sound genuine. They will also often try to rush or panic their potential victims into making a payment, for example by claiming their money is at risk or their account will be blocked unless they act.

The banking and finance industry has put in place a range of measures to combat impersonation scams. This includes the Banking Protocol, a scheme that allows bank branch staff to alert police to suspected scams and which prevented £19 million of fraud and led to over 100 arrests in the first half of this year. The industry is also working closely with Ofcom to crack down on number spoofing and with the mobile phone industry to block scam text messages including those exploiting the Covid-19 crisis.

UK Finance is also urging the public to follow the advice of the Take Five to Stop Fraud campaign, which offers straight-forward and impartial advice to help people spot scams and protect themselves against fraud.

STOP

If you receive a request to make an urgent payment, change supplier bank details or provide financial information, take a moment to stop and think.

CHALLENGE

Could it be fake? Verify all payments and supplier details directly with the company on a known phone number or in person first.

PROTECT

Contact your business's bank immediately if you think you've been scammed and report it to Action Fraud.

TAKE FIVE TO STOP FRAUD™

Forward any suspicious emails to **report@phishing.gov.uk**

Report suspected scam texts to your mobile network provider by **forwarding them to 7726**

CALL ESSEX POLICE 101

IN AN EMERGENCY ALWAYS CALL 999

Keep up to date with fraud and do *even more* Online at essex.police.uk