UPDATE FROM MET POLICE CYBER CRIME UNIT – November 2020

**Online Banking -**the use of online banking or Smartphone/Tablet banking apps has grown. To stay safe banking online, protect your password and personal details to stop criminals accessing your accounts. Many banks provide one-time passcodes sent to your device when setting up payments. Never share these with anyone, even the bank. If you’re speaking to your bank on the phone, and you are asked for it, you are speaking to a criminal, not your bank. So, to protect yourself:

* Choose, use and protect passwords and memorable words with great care.
* Watch a video on passwords at [www.met.police.uk/littlemedia](https://eur02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.met.police.uk%2Flittlemedia&data=04%7C01%7Ctracy.c.homewood%40met.police.uk%7Cc6bd1195c92c4ae9e66b08d87fe656a1%7Cf3ee2a7e72354d28ab42617c4c17f0c1%7C0%7C0%7C637399976673102513%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=ZYjT%2FmNTESkspg2eKQSane8ryhCutcw17Jw0vj5vi2Q%3D&reserved=0) for further advice;
* Keep online banking software and banking apps up to date;
* If logging in whilst in public, shield any PIN codes or passwords;
* Always log out of online banking or a banking app when finished. Closing the app or web page or turning off your device may not be sufficient;
* Do not use public Wi-Fi for banking. It’s very difficult to tell if a hotspot is secure;
* Don’t share security codes with anyone.

If your bank has called you, take a reference number, and hang up before recalling on a number you know to be safe after a few minutes to clear the line.

**Advance Fee Fraud -**is an umbrella term to describe a particular fraud type where the criminal convinces a victim to make upfront payments for goods, services or financial gains that don’t exist. The criminal will offer something to you but, in order to progress, you’ll need to pay something up front. This list of types of Advance Fee Fraud is not exhaustive:

**Clairvoyant or Psychic Fraud**– The criminal predicts something significant in your future but needs money to provide a full report;

**Cheque Overpayment Fraud** – The criminal overpays for something with an invalid cheque, and asks for change;

**Fraud Recovery Fraud** – Once you’ve been a victim of fraud, the criminal contacts you claiming they can recover your losses, for a fee;

**Inheritance Fraud** – The criminal tells you you’re in line to receive a huge inheritance but you’ll need to pay a fee to release the funds;

**Loan Fraud**– The criminal asks you to pay an upfront fee for a loan;

**Lottery Fraud** – You’re told you’ve won a prize in a lottery but you’ll need to pay the criminal an admin fee;

**Racing Tip Fraud** – The criminal offers racing tips “guaranteed” to pay off, for a fee;

**Rental Fraud** – The criminal asks for an upfront fee to rent a property that may not be theirs, or even may not exist.

**African Letter Fraud (aka 419 Fraud)** – The criminal asks for help moving money from one country to another, promising to cut you in, but asks for a payment upfront;

**Work from home Fraud** – The criminal offers you to make easy money working from home but you need to pay a fee in advance, for business leads, or a website;

**Vehicle Matching Fraud** – The criminal contacts you after you placed an advert to sell something (usually a car) and asks for a “refundable” fee to put you in touch with a non-existent buyer. To protect yourself:

* Be extremely wary about giving money to anyone upfront;
* If they claim to be an official, double check their identity, but don’t do so using any contact details they give you;
* Don’t be pressured into making a decision.

**Investment Fraud -**Investing in stocks and shares or other commodities can be a successful way of making money but it can also lead to people losing their entire life savings. Fraudsters persuade you to invest in all kinds of products offering high rates of return, particularly over longer time periods, that do not exist. Common products include binary options, virtual currency, carbon credits, wine, rare metals, land, gemstones and alternative energy. Initial investments will often yield small returns as an incentive to invest further; however, larger investments or cashing out will be met with excuses or a penalty charge. Eventually, contact will be impossible and all funds and bogus returns lost. Fraudsters are organised and may know of your previous investments or share purchases. Knowing this does not mean they are genuine. Criminals direct you to well-presented websites or send you glossy marketing material. These do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

It’s easy to register a company with Companies House. This does not confirm or endorse they can provide genuine investments. Indeed, emerging investment markets may be unregulated, making these open to abuse. Companies may be registered at prestigious addresses, e.g. Canary Wharf or Mayfair. This does not mean they operate from there. It’s an accepted business practice to rent a virtual office to enhance a business’s status. Fraudsters exploit this. The fraudster may put pressure on you by offering a ‘once in a lifetime opportunity’ or claim the deal has to be done quickly to maximise profit. In addition, be wary of companies that offer to ‘recover’ funds you lost to any sort of scam. It may be linked to the company that initially defrauded you and is targeting you again. To protect yourself:

* If it sounds too good to be true, it probably is;
* Genuine investment companies will not cold call you
* Research what you are offered and the investment company;
* Speak to Trading Standards if you have concerns;
* Before investing, check the Financial Conduct Authority register ([https://register.fca.org.uk/](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fregister.fca.org.uk%2F&data=04%7C01%7Ctracy.c.homewood%40met.police.uk%7Cc6bd1195c92c4ae9e66b08d87fe656a1%7Cf3ee2a7e72354d28ab42617c4c17f0c1%7C0%7C0%7C637399976673112472%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Fp7wA9vz2ReDz0PUy5HpidgT7dEdwejsLHopz%2FlznfA%3D&reserved=0)) to see if the firm or individual is authorised
* Check the FCA Warning List of firms to avoid.

**Push Payment Fraud -**Criminals pretend to be from somewhere official, for example, your bank or the tax office. They contact you via email, phone or social media and warn you of fake, suspicious or criminal activity on your bank account. They state they’ve set up a safe account for you to transfer your funds into but this is actually their account. To protect yourself:

* Be suspicious of a call out of the blue from someone claiming to be from a position of authority;
* Take down the person’s name, authority, department, branch etc. and verify using independent source contact details;
* A genuine official from the Police, your bank, HMRC or any other trusted authority will NEVER call you to ask you to verify your personal banking details, PIN or password, or threaten you with arrest;
* Never transfer money into another account unless you are 100% certain of the owner of the account;
* Your bank will never set up a “safe” account for you;
* If you are a victim, contact your bank immediately, as it may be able to help;
* Watch a video on Impersonation Fraud at [www.met.police.uk/littlemedia](https://eur02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.met.police.uk%2Flittlemedia&data=04%7C01%7Ctracy.c.homewood%40met.police.uk%7Cc6bd1195c92c4ae9e66b08d87fe656a1%7Cf3ee2a7e72354d28ab42617c4c17f0c1%7C0%7C0%7C637399976673112472%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=VWiOwmMhKAlBn3OVSWzSN8ptDsCPlVuZrJdyGCfaCdw%3D&reserved=0).

**Consumer Investment Fraud -**Businesses use deceptive practices that cause victims to suffer financial losses. Victims believe they are participating in a legal, valid transaction when they are actually being defrauded. Fraud against consumers is often related to false promises or inaccurate claims made to consumers as well as practices that directly cheat consumers out of money. To protect yourself:

* Research the company before purchasing goods or services;
* Use Companies House to find out how long they have been trading;
* Ensure you use trusted, reviewed companies;
* Avoid using direct bank transfers when purchasing online, use a credit card.

Your bank, the police, or tax office will **never** ask you to attend your bank, withdraw, transfer or pay money over the phone or send couriers to collect your card or cash. Nor would they ask you to buy goods or vouchers. Always report, Scams fraud and cyber crime to Action Fraud online at [**www.actionfraud.police.uk**](https://eur02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.actionfraud.police.uk%2F&data=04%7C01%7Ctracy.c.homewood%40met.police.uk%7Cc6bd1195c92c4ae9e66b08d87fe656a1%7Cf3ee2a7e72354d28ab42617c4c17f0c1%7C0%7C0%7C637399976673122425%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=5RHYkqGd1j%2B1N%2BzFqTz5FI1Ut9fe4RHkvxMVfk76JYg%3D&reserved=0)or telephone on 0300 123 2040.