INFORMATION SHEET
V1/2025 - FRAUDS AND SCAMS

TYPES OF FRAUDS AND SCAMS

Scammers are always looking to separate you from your money in your personal and your business transactions. Scams are becoming highly elaborate and more sophisticated every day.

They often target you through social engineering (methods used to manipulate people to carry out specific actions or share confidential information). They will contact a potential victim, such as you, after gathering information about you from a variety of places, such as your social media profiles, and even by the websites you have visited.

If you believe you may have been scammed, contact us at compliance@alt21.com as soon as reasonably possible.

Protect yourself from scams and fraud by gaining a deeper understanding of the current trends below:

- **Investment scams**
- **Identity theft**
- **Phishing or spoofing**
- **Online relationship scams**
- **Invoice scams**
- **Payroll scams**
- **Tips on how to protect yourself from being a victim**

INVESTMENT SCAMS

Investment Scams Fraudsters lure victims with seemingly incredible investment opportunities that promise guaranteed returns.

Red Flags:

- **Promises of low-risk, high-return investments**
- **Unsolicited communication**
- **Aggressive sales tactics**
- **Pressure to make immediate financial decision**

IDENTITY SCAMS

Identity theft involves the theft of your personal information, including your name, date of birth, or address.

Criminals steal your personal information to commit fraud, potentially:

- **Access and drain your bank account**
- **Open new bank accounts in your name and take out loans**
- **Purchase expensive goods in your name**
- **Access your email or social media accounts**

Red Flags:

- **You notice unexpected large sums of money missing from your bank account.**
- **You receive invoices or receipts addressed to you for goods or services you didn't purchase.**
- **You can't log in to your social media or email accounts.**

PHISHING OR SPOOFING

Phishing or spoofing involves the scammer sending you fraudulent communications mimicking legitimate businesses aim to extract your personal information. This is an attempt to "phish" for your personal information, including your address, your login passwords, your phone number, and even your banking details.

Phishing or spoofing scams are designed to look genuine and often copy the format used by the company the scammer is pretending to represent.

Red Flags:

- **Sender address is unusual, misspelt or slightly different from the correct address**
- **The email or SMS doesn't address you by your proper name**
- **Poor grammar and spelling**
- **Appear to come from familiar organisations or a business you regularly deal with, asking you to update or verify your details**

ONLINE RELATIONSHIP SCAMS

Criminals exploit emotional connections on dating platforms by gaining your trust, and then they will ask you for money, gifts, or your personal details, or to cover the costs of a supposed personal or family emergency.

Red Flags:

- **Quickly moving communication to private channels**

- They start asking you personal questions about your finances early on in the relationship or conversation
- Their profile on the dating website is not consistent with their social media accounts or what they've told you
- Requesting financial assistance, i.e. asking you to buy certain goods and send them somewhere, or accept money into your bank account and transfer it somewhere else
- Fabricating personal emergencies

INVOICE SCAMS

Scammers are impersonating your suppliers or employees to:

- Request payment to new bank accounts
- Alter existing payment details
- Create seemingly legitimate payment requests

As the invoice looks legitimate, is sent from a compromised but genuine email address, and is made to look like someone you know, they can be harder to identify. You can contact your supplier directly to double check, using the details you have on file and not those on the invoice.

Red Flags:

- The supplier has provided new bank account details
- The supplier has asked you to cancel the most recent payment and send funds to a new account
- Urgent payment is requested
- The payment details on the invoice have been altered
- Be wary of invoices from a supplier you haven't dealt with in a while, or a larger payment amount than usual

PAYROLL SCAMS

Payroll scams involve scammers impersonating employees, and sending an email from a legitimate but compromised email address, or a message via social media, to their employer requesting an update to their bank account details.

Red Flags

- The sender's email address looks very similar to the staff members, but with a slight variation, for example, the addition of numbers at the end
- Unusual message or request to change account details or payment to a new bank account

TIPS ON HOW TO PROTECT YOURSELF AGAINST BEING A VICTIM

Cybersecurity and Fraud Prevention:

- **Stay alert and sceptical. Ignore suspicious emails or text messages and avoid clicking on any links.**
- **Create robust, unique passwords with two-factor authentication for all accounts.**
- **Consistently monitor your bank accounts for suspicious or unauthorized transactions.**
- **Implement two-factor authentication across email and banking platforms.**
- **Refrain from opening attachments from unknown senders.**
- **When uncertain about a message's legitimacy, access accounts through your standard login method.**
- **Protect your personal identification numbers and documents from unverified sources.**
- **Fortify your digital environment with comprehensive anti-virus software and strong firewalls.**
- **Minimise use of public computers and unsecured Wi-Fi networks for sensitive activities.**
- **Carefully manage your online presence and social media information sharing.**

Investment Fraud Protection:

- **Be wary when receiving unsolicited emails, or phone calls.**
- **Do not be pressured to make a quick decision about your money or investments, and never commit to an investment on the spot.**
- **Research before you commit to any investments, and take the time to seek. independent professional, financial or legal advice. For instance check who owns the company, how it recently performed on the stock exchange, and whether it is authorised to sell you investment products and has a financial services licence.**
- **Take the time to understand a company's business and its products or services before investing**
- **Be wary of offshore investments. If something goes wrong, it's harder to trace money sent abroad**
- **Look out for grammatical mistakes in the email address, recipient name or website**

Invoice Fraud Prevention:

- **Meticulously compare new payment details against historical transaction records Check and look out for any changes .**
- **Contact your vendor to verify the change using a phone number you already have on file. Don't rely on the contact details on the invoice.**
- **Try to limit the number of people in your business who are authorised to make orders or pay invoices. Consider having an extra person to approve payments to new accounts or for larger transactions.**
- **Be cautious about how you contact a business. The best defence is to assume the email is untrustworthy and to contact the business directly through channels you trust.**

Online Relationship Safety:

- **Thoroughly investigate online profiles through comprehensive internet searches.**
- **Do an internet search of different elements of the person to help determine if they are who they say they are**
- **Be on alert for grammar mistakes or inconsistencies in the stories of people you speak to online**
- **Be very very wary of any requests for financial assistance Do not give money without properly checking. Speak with friends and family.**
- **Cross-reference profile information across multiple online platform using video calls such as Skype, Facetime or Zoom.**

— END