Anti-Scam & Fraud Prevention

Financial fraud and scams are becoming increasingly sophisticated. Criminals often rely on urgency, impersonation, and manipulation to convince people to send money or reveal sensitive information.

At **Cepheus Pay**, protecting our clients is a priority. This page explains how fraud and scams work, how to recognize them, and what to do if you believe you may have been targeted.

If something feels suspicious, **always pause and verify before taking action.**

What Is Fraud

Fraud occurs when someone gains access to your financial information or account **without your permission** and uses it to perform unauthorized transactions.

Fraud typically involves criminals stealing credentials, payment details, or personal information in order to access financial services.

Examples may include unauthorized transactions, stolen card details, or criminals accessing an account using compromised login credentials.

Types of Fraud

Financial fraud can take several forms, including the following.

Account Takeover Fraud

Criminals gain access to your account by obtaining login credentials through phishing, malware, or data breaches.

Once access is obtained, they may:

- Transfer funds
- Change account settings
- Attempt unauthorized transactions

Card or Payment Fraud

Fraudsters obtain payment details and use them to conduct unauthorized purchases or transfers.

This may occur through:

- Data breaches
- Skimming devices
- Phishing attacks
- Malware on compromised devices

Identity Theft

Criminals use stolen personal information to impersonate another individual.

This may involve opening financial accounts, applying for services, or conducting transactions using someone else's identity.

What Is a Scam

A **scam** is a form of financial crime where criminals manipulate victims into **voluntarily sending money or sharing sensitive information**.

Unlike traditional fraud, where criminals secretly steal information, scams rely on **social engineering** - psychological tactics used to gain trust or create urgency.

Scammers may pretend to be:

- A financial institution or payment provider
- Government authorities or law enforcement
- A well-known company or service provider
- A friend, colleague, or family member
- An investment advisor or recruiter

Their objective is usually to pressure victims into making payments or revealing sensitive information before verifying the request.

Types of Scams

Scams can take many forms. Below are some of the most common types affecting online financial services.

Impersonation Scams

A fraudster pretends to represent a trusted organization such as a bank, payment provider, government authority, or courier service.

Common examples include messages claiming:

- Your account has been compromised
- You must urgently verify your identity
- A payment problem must be resolved immediately
- You need to move funds to a “secure account”

Important:
If anyone asks you to move money to a **“safe” or “secure” account**, it is almost certainly a scam. Legitimate financial institutions do **not** ask customers to move funds to protect them.

Phishing Scams

Phishing involves fraudulent emails, text messages, or websites designed to steal login credentials or personal data.

These messages may:

- Contain links to fake login pages
- Ask you to confirm account details
- Claim that your account is restricted or under review
- Encourage you to download software or attachments

Never enter your login credentials on websites reached through suspicious links.

Investment and Crypto Scams

Fraudsters promote “exclusive” investment opportunities promising guaranteed profits.

Warning signs include:

- Guaranteed or unusually high returns
- Pressure to invest immediately
- Requests to transfer funds to personal accounts
- Fake trading dashboards showing fabricated profits

Legitimate investments always involve risk and **do not guarantee returns**.

Job or Task Scams

Victims are offered easy online work such as reviewing products or completing small digital tasks.

The scam often works like this:

1. The victim initially receives small payments.
2. They are told they must deposit funds to unlock higher earnings.
3. Additional payments are requested.
4. The money cannot be withdrawn.

Purchase and Marketplace Scams

Fraudsters advertise products online at unusually low prices.

After payment is sent:

- The item never arrives
- The seller disappears
- The payment cannot be recovered.

Rental Scams

A scammer pretends to be a landlord offering attractive rental properties.

Warning signs include requests for deposits before viewing the property or pressure to send payment quickly.

Romance Scams

A fraudster builds an online relationship over time and later asks for financial assistance.

These scams often rely on emotional manipulation.

Delivery Scams

You receive a message claiming a package cannot be delivered until a small fee is paid.

The message may contain fake courier websites or links requesting payment information.

Charity Scams

Fraudsters create fake charities or impersonate real organizations during disasters or crises.

Always verify the organization before donating.

Advance Fee Scams

Victims are told they will receive a large payment, inheritance, or loan but must first pay a processing or administrative fee.

After the fee is paid, the promised funds never arrive.

How to Tell It’s a Fraud or a Scam

Scammers often rely on psychological pressure and manipulation.

Be cautious if you encounter the following warning signs.

Urgency and Pressure

Messages insisting you act immediately.

Examples:

- “Your account will be closed today.”
- “You must move funds immediately.”
- “Failure to act will result in penalties.”

Requests for Secrecy

Fraudsters may ask you not to contact anyone else or to keep the situation confidential.

Requests for Security Information

No legitimate financial service will ask you to share:

- Passwords
- Authentication codes
- Two-factor verification codes
- Account recovery information

Requests to Install Software

If someone asks you to install remote-access software so they can “assist” with your account, this is likely a scam.

Requests to Move Funds to a “Safe Account”

Legitimate financial institutions **never ask customers to move funds to another account for security purposes.**

Protect Your Cepheus Pay Account

You can reduce the risk of fraud and scams by following basic security practices.

Recommended measures include:

- Never share authentication codes
- Use strong and unique passwords
- Avoid logging in through links received in emails or messages
- Verify unusual requests through official support channels

If you believe your login credentials may have been exposed, change your password immediately and @contact support.

What to Do If You've Been Scammed or Suspect Fraud

If you suspect fraud or believe you have been targeted by a scam, act quickly.

---

1. Stop all communication

Do not send additional funds or continue communicating with the suspected scammer.

2. Secure your account

Immediately:

- Change your password
- Reset two-factor authentication
- Remove any unknown devices or sessions
- Scan your device for malware if you installed any software

---

3. Contact Cepheus Pay Support

If a suspicious or fraudulent transaction may have occurred, @contact our support team as soon as possible.

Provide any relevant information, such as:

- Transaction amount and currency
- Recipient details
- Date and time of the transaction
- Screenshots of messages or emails
- Any links or websites involved

Our team will review the situation and take appropriate steps where possible, including investigating suspicious activity and providing guidance on next actions.

Early reporting significantly increases the chances of identifying and responding to fraudulent activity.

---

4. Report the Scam to Local Authorities

If you have suffered a financial loss, suspect fraud, or believe that a criminal offence may have occurred, you should report the matter without delay to your local police and, where relevant, to the applicable national fraud reporting authority, including the Canadian Anti-Fraud Centre (CAFC) https://reportcyberandfraud.canada.ca for Canada and Action Fraud https://www.reportfraud.police.uk for the United Kingdom.

---

5. Monitor Your Financial Activity

If personal or financial information may have been exposed:

- Monitor your accounts for unusual activity
- Review your transactions

If You Are Unsure

If you receive a message or request that appears suspicious, the safest action is to **pause and verify before proceeding**.

Contact Cepheus Pay through official @support channels and our team will help you confirm whether the request is legitimate.

Protecting your financial security starts with awareness - and we are here to help when you need it.