Olympiade Internationale sur la Securité Financière

Face sombre de IA

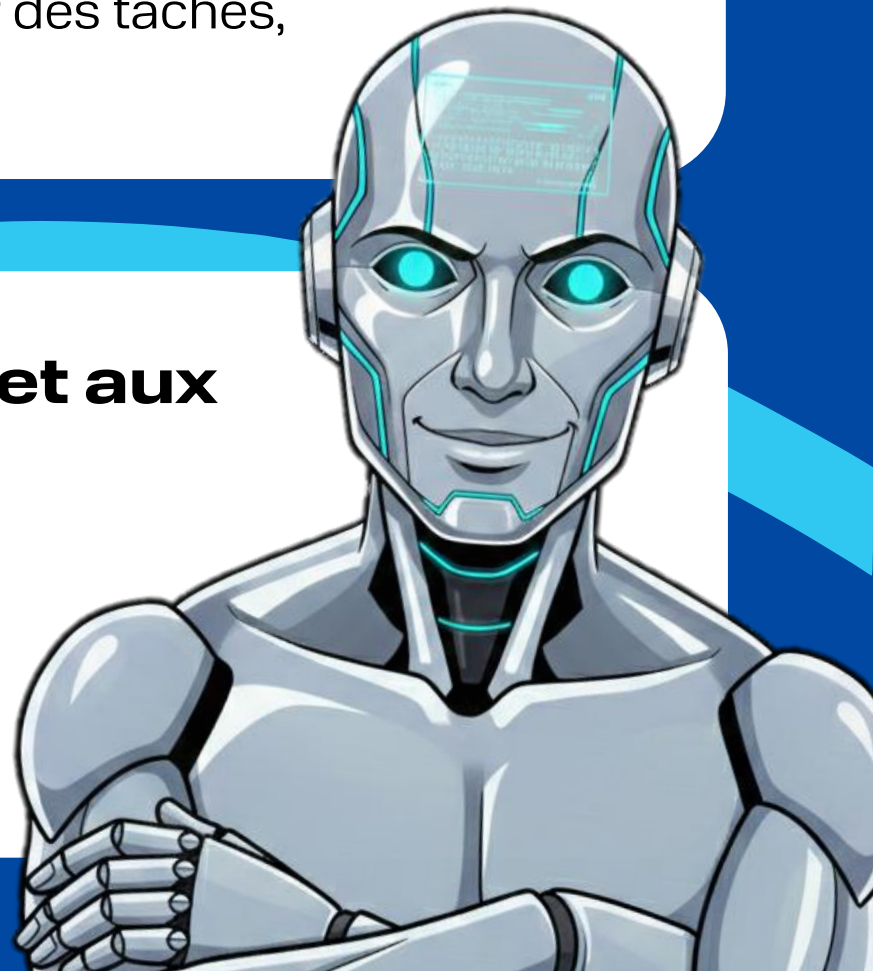
Intelligence Artificielle

Intelligence artificielle (IA) Artificial intelligence

systèmes informatiques capables d’accomplir des tâches, associées à l'intelligence humaine

IA — ensemble de technologies qui permet aux systèmes de

- comprendre des requêtes formulées en langage naturel
- analyser, traiter et extraire des données pertinentes
- reconnaître des formes, des symboles et des régularités
- apprendre à partir de flux massifs de données
- prendre des décisions et s’adapter à des contextes variés



Domaines d’applications de l’IA

Médecine et santé

- Traitements personnalisés
- Développement de médicaments
- Analyse de données

Secteur bancaire

- Investissements automatisés
- Score de crédit et évaluation des risques
- Prise de décision en temps réel

Éducation

- Adaptation des contenus pédagogiques à l’élève
- Identification des lacunes de connaissances
- Préparation d’exercices personnalisés

Science et recherche

- Identification rapide de régularités
- Optimisation des cycles de recherche
- Recherche de solutions par l'analyse

Protection de la cybersécurité

Comment l’IA lutte contre la fraude ?

- détecte et intercepte les schémas frauduleux
- réduit la pression sur les victimes réelles

Exemple : « Cyber-grand-mère » — modèle de l’IA développé par un opérateur mobile

- mène une conversation avec des fraudeurs en se faisant passer pour une cliente âgée
- détourne l’attention des malfaiteurs de vraies personnes, leur fait perdre du temps et des ressources

Envers de l'IA

Menaces financières

- Essor de la cybercriminalité basée sur l'IA
- Vols de fonds et de données
- Automatisation des schémas criminels

Zones à risque particulier

- Hausse du nombre de victimes mineurs
- Attaques par appels et messages (écoles, administrations, opérateurs)
- Fraude liée à la vente ou à l'achat de comptes de jeux et de réponses aux examens d'État

Opérations non consenties par les clients

27,5 Mrd RUB
2024

21 Mrd RUB
9 mois de 2025

Détournements évités

222 Mrd RUB
Novembre 2025

Prévention

- Rosfinmonitoring
- Cellules de renseignement financier de la CEI
- Groupe eurasien (EAG)

Blanchiment de capitaux

Cyberfraude

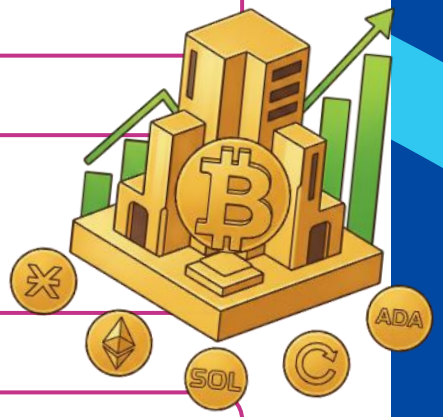
Comptes de prête-nom

virements multiples,
mixage de fonds

Brouillage des pistes financières

Plateformes crypto

Légalisation / financement d'activités criminelles



La menace est de nature transnationale

Qu'est-ce qu’une mule financière (dropper)?

Mule financière (Dropper)

Une personne qui utilise ses propres cartes bancaires pour retirer ou transférer (faire transiter) des fonds d’origine criminelle

Implication des jeunes

Qui est impliqué ?

- Adolescents dès 14 ans
- Étudiants et écoliers
- Personnes sans emploi

Plus d’un million de mules financières

L'ampleur du problème en Russie

Selon la Banque de Russie

Comment on recrute ? Astuces psychologiques:

- **Urgence** — «aujourd’hui seulement»
- **Simplicité** — «chacun peut le faire»
- **Fausse légalité** — «c’est tout à fait légal »
- **Progressivité** — des petits montants vers les gros
- **Preuve sociale** — «des centaines nous ont déjà rejoints »

Responsabilité

Responsabilité pénale directe

prévue pour la fraude à la mule (dropping) par le complément à l'article 187 du Code pénal

Peine

- jusqu' à **3 ans d'emprisonnement** — pour le transfert de données bancaires
- jusqu' à **6 ans d'emprisonnement** — pour les organisateurs (recruteurs de mules financières /droppers)

Pratique judiciaire

- En 2025, première poursuite pénale contre un recruteur de mules financières /droppers
- Coopération avec le ministère de l'Intérieur— motif d'exemption de poursuites
- Organisateur identifié grâce au témoignage d'une mule (dropper) arrêté

Deepfakes : une nouvelle menace

Deepfake

(de l'anglais deepfake – « contrefaçon profonde »)

une vidéo, un enregistrement audio ou une photo créés grâce à des techniques de l'IA, où une personne fait ou dit quelque chose qui n'a jamais eu lieu en réalité

Comment ça fonctionne ?

- Appels déguisés en sondages pour enregistrer la voix
- IA copie le visage et la voix d'une personne
- Création de deepfakes vocaux

Quelques secondes d'enregistrement
pour créer un deepfake vocal

Première affaire retentissante

2019, Royaume-Uni

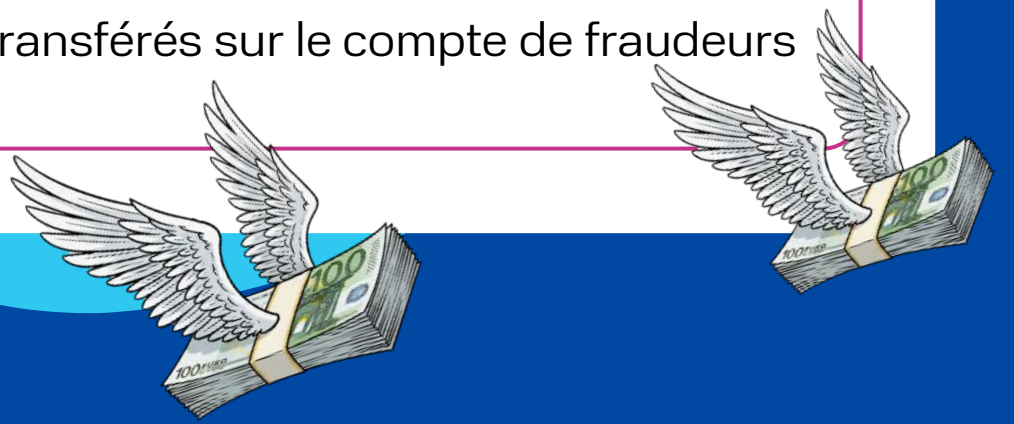
des escrocs ont copié la voix du PDG d'une entreprise énergétique à l'aide de l'IA

Schéma d'attaque

« La voix du PDG » appelle un subordonné avec un ordre urgent de transférer des fonds sur le compte d'un fournisseur

€220 000

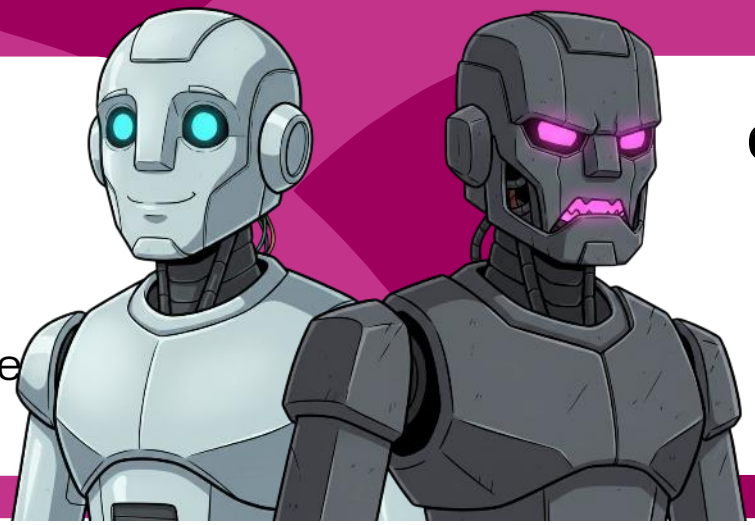
sont transférés sur le compte de fraudeurs



«Jumeau maléfique » (Evil Twin)

Principe de l'attaque

Un réseau Wi-Fi factice copiant un réseau légitime



Que dérobe-t-on ?

- Noms d'utilisateur et mots de passe
- Données de cartes bancaires
- Correspondances et historique de navigation

Comment fonctionne le schéma?

Clonage du réseau
même SSID, signal plus fort

→

Connexion de la victime
cafés, aéroports, centres commerciaux

→

Homme du milieu
interception du trafic

→

Phishing
fausse page de connexion

« Jumeau maléfique » à l'aéroport

Situation

- Une écolière s’est connectée à un Wi-Fi portant le nom de l'aéroport
- Le réseau figure en tête de liste
- Le code s'est avéré être un mot de passe à usage unique

Erreurs critiques

- Avertissements ignorés concernant un réseau non sécurisé
- Numéro de téléphone saisi
- Code déjà saisi issu d'une messagerie

Résultat

- Perte d'accès à la messagerie
- Compromission des données personnelles

Attention !

Les codes issus des messageries ne sont jamais demandés lors d'une connexion Wi-Fi

IA–phishing

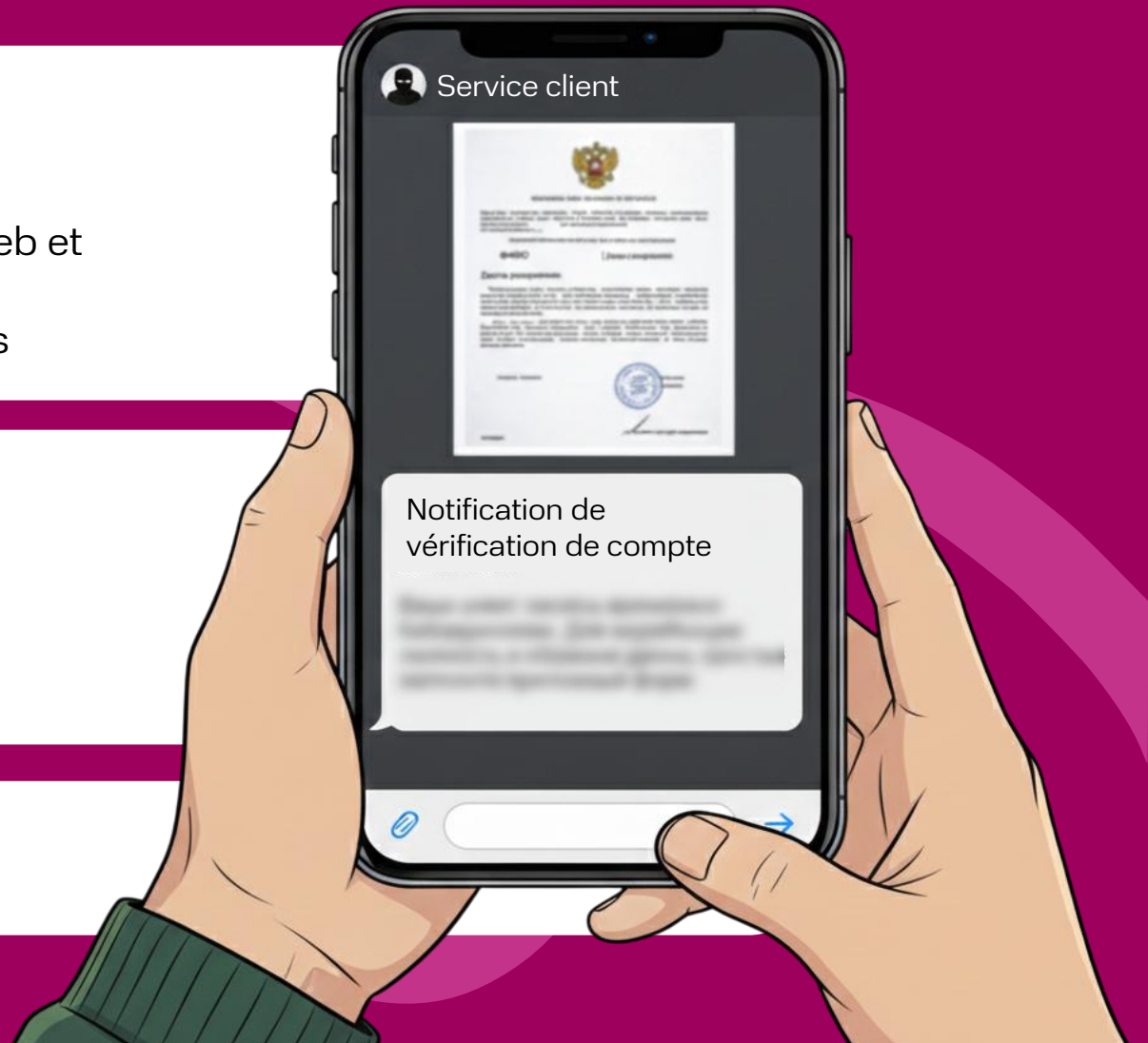
Avant de commencer à travailler avec l'IA

- analyse les données issues des réseaux sociaux, sites web et fuites d'informations
- génère des messages et courriels parfaitement crédibles

Envoie un message personnalisé

- sans erreurs et sans formules génériques
- ressemble à une véritable communication professionnelle

Résultat – perte d'argent



IA-vishing

IA-vishing

(англ. vishing = voice + phishing): hameçonnage vocal

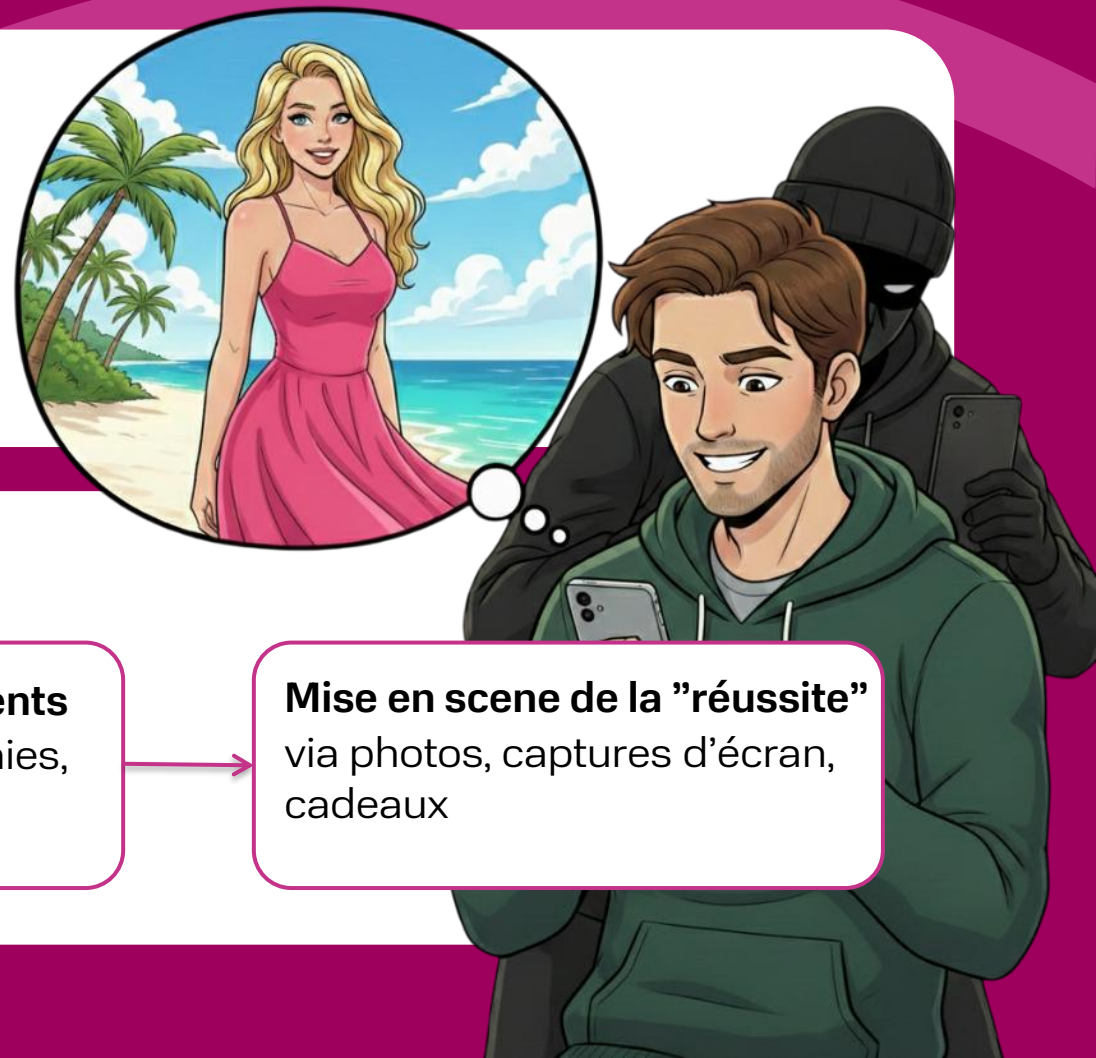
- variante vocale du deepfake
- l'IA reproduit une voix à partir de quelques secondes d'enregistrement
- permet de dialoguer avec la victime

l'IA rend la fraude terriblement réaliste

Arnaque sentimental

Principe de l’attaque

- L’IA mène des conversations avec des milliers de personnes simultanément
- Crée une illusion de confiance, exploite les données des reseaux sociaux pour personnaliser les échanges



Fonctionnement du stratagème

Échanges dans le chat
questions personnelles, messages vocaux

→

Proposition d‘investissements
Paris sportifs, cryptomonnaies, systèmes pyramidaux

→

Mise en scene de la ”réussite”
via photos, captures d’écran, cadeaux

Sécurité sur Wi-Fi public

Évitez les reseaux non securisés

Les ”jumeaux maléfiques” sont presque toujours ouverts

Ne saisissez jamais vos mots de passe ni vos données bancaires

Un Wi-Fi public peut intercepter votre traffic

Utilisez uniquement des sites HTTPS

Icône du cadenas→ connexion chiffrée de bout en bout

Soyez attentif aux avertissements

Ils signalent une menace réelle

Activez l’authentification multifacteur (MFA)

Mot de passe+ code à usage unique

Ne cédez pas à la panique!

Un moyen simple, mais efficace, de se protéger contre l'usurpation de voix par l'IA

1. **Raccrochez** au moindre doute
2. **Rappelez votre proche ou ami**
   à partir du numéro enregistré dans vos contacts
3. **Utilisez un mot faisant partie du code familial**
   pour confirmer l'identité
4. **Posez des questions personnelles** que seul

vos proches peuvent connaître

Respectez l'hygiène numérique !

Comment empêcher l'IA de cloner votre voix

- **Limitez l'accès à vos réseaux sociaux** *(réservé aux amis)*
- **Ne publiez pas d'enregistrements de votre voix en accès libre** (statuts, streams, messageries)

Contrôlez votre état émotionnel !

- Toute information qui suscite une forte émotion et exige une action immédiate est très probablement une tromperie
- Parlez-en avec vos proches

Esprit critique-arme absolue

N'oubliez pas : les institutions publiques (Banque centrale, services de sécurité, administration fiscale) ne règlent pas les « questions importantes » par telephone.

Coupez les contacts suspects !

Que faire en cas d'arnaque :

- **Interrompez immédiatement** l'échange dès qu'il est question d'argent, de paris ou de cryptomonnaies
- **Faites preuve d'esprit critique**
- **Bloquez** l'escroc
- **Ne transférez jamais l'argent** à une personne que vous n'avez pas rencontrée dans la vrai vie.
- **Si nécessaire**, signalez l'incident aux autorités compétentes et à l'administration de la plateforme

L'arnaque sentimentale est un jeu de confiance

dont la mise finale, c'est votre argent.

Les droppers — intermédiaires dans les montages financiers frauduleux

Qui sont les droppers

- des personnes qui reçoivent de l'argent volé
- ils transfèrent ou retirent des fonds pour les organisateurs
- ile remettent leur carte ainsi que l'accès à la banque en ligne

Les droppers participent à une infraction pénale

Acquisition ou cession d'une carte bancaire par une personne non-cliente de l'établissement émetteur » — cette infraction est passible d'une peine d'emprisonnement pouvant aller jusqu'à 6 ans, assortie d'une amende.

Article 187 du Code pénal de la fédération de Russie
« Trafic illicite d'instruments de paiement »

⇆Statistiques sur les droppers en Russie✕

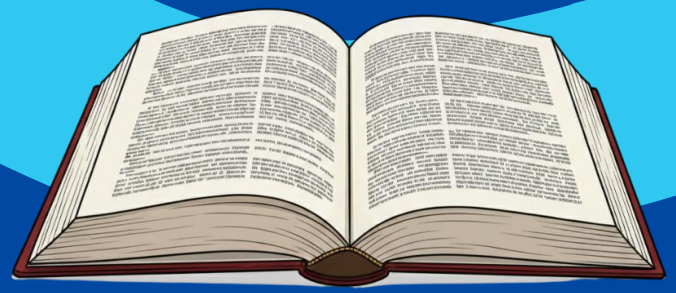
> 1 mln
de clients-« droppers »
dans les banques

~ 20%
sont des adolescents
inconscients des
conséquences

Les droppers constituent le maillon clé dans le blanchiment des fonds volés

risque une pénalisation au titre de **l'article 174 du Code pénal de la Fédération de Russie :**
« Blanchiment d'argent ou d'autres biens acquis par autrui de manière criminelle ».

Sensibilisation et vigilance sont essentielles



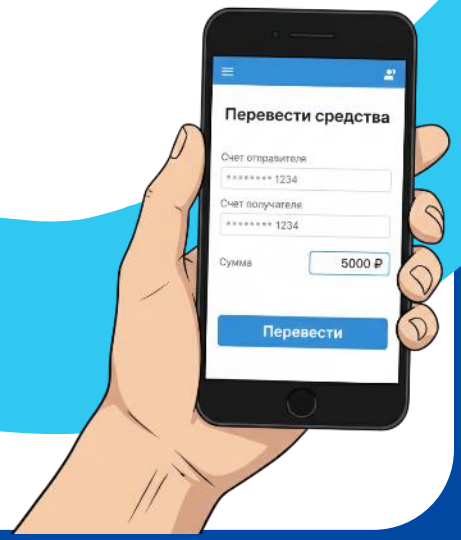
⇆ Types de droppers selon leur rôle ✕

Déverseurs

- reçoivent des espèces →
- les déposent sur un compte →
- les transfèrent vers d'autres comptes

Transitaires

- reçoivent des virements →
- les redirigent vers d'autres comptes ou portefeuilles



Retireurs

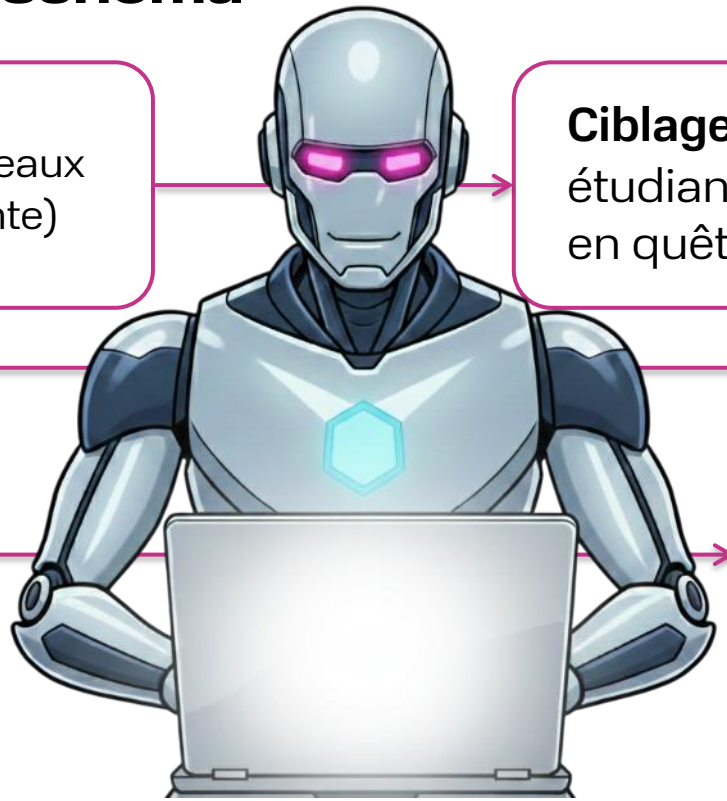
- retirent l'argent aux distributeurs →
- le remettent en mains propres aux organisateurs

Recrutement de drops via l'IA

Comment fonctionne le schéma

Réseaux neuronaux et NLP
analysent les sources ouvertes (réseaux sociaux, forums, plateformes de vente)

Ciblage des groupes vulnérables
étudiants, personnes sans emploi en quête d'un « revenu facile »



Évaluation psychologique de la victime
publications, style de communication → suggestibilité, appât du gain

Premier contact
Chatbots, utilisation d'avatars deepfake

« Un petit job facile »

Scénario typique

- sans expérience ni diplôme
- travail depuis chez soi, 2–3 h par jour
- condition requise : une carte bancaire ou un accès à la banque en ligne

La personne devient, sans le savoir, une mule financière et complice d'une infraction

« Le virement erroné »

Comment fonctionne le schéma

Le virement « erroné »

arrive sur le compte

→

Un appel demandant

de rembourser de toute urgence l'argent sur le bon compte

→

Transfert d'argent

sur les coordonnées des fraudeurs

La seule et unique solution

- Contacter immédiatement la banque
- Suivre strictement ses instructions

SMS de : Numéro inconnu
Montant : 50 000 RUB

J'ai envoyé par erreur, veuillez retransférer l'argent sur ce numéro

« Administrateur de loterie »

Comment se déroule le recrutement

- On vous propose un « travail technique »
- Votre mission : distribuer les gains aux «gagnants»

Ce qui se passe en réalité

- La personne recrutée devient un dropper (mule financière)
- L'argent sur le compte provient d'autres victimes
- Les transferts sont présentés comme des « gains »,

mais partent :
— vers d'autres droppers ou des prête-noms
— directement vers les fraudeurs

Rôle clé du dropper

- Il fragmente et « nettoie » les flux financiers criminels
- Il complique considérablement la détection du système par les banques et les forces de l'ordre

Recrutement via les réseaux sociaux

Comment la victime est ciblée

- L'IA analyse les réseaux sociaux : publications sur la recherche d'emploi, participation à des tirages au sort
- Les personnes vulnérables sont sélectionnées

Légendes typiques

• « Gestionnaire de dons »
• Assistant d'un blogueur ou d'un streameur
• Bénévole acceptant des donations

Comment se déroule le recrutement :

• Un compte « vivant » avec des photos volées
• Messages proposant un petit boulot, de l'aide, un projet « social »
• On vous persuade de la légalité du système
• On vous demande de transférer l'argent via votre carte personnelle

Aucune organisation légale n'utilise la carte d'une personne prise au hasard

Responsabilité pénale en Fédération de Russie

Articles prévoyant des sanctions pour le dropping (activité de mule financière)

- Art. 174 du Code pénal « Légalisation (blanchiment) de fonds ou d'autres biens acquis par d'autres personnes par voie criminelle »
- Art. 187 du Code pénal « Trafic illicite de moyens de paiement »
- Art. 159 du Code pénal « Fraude »

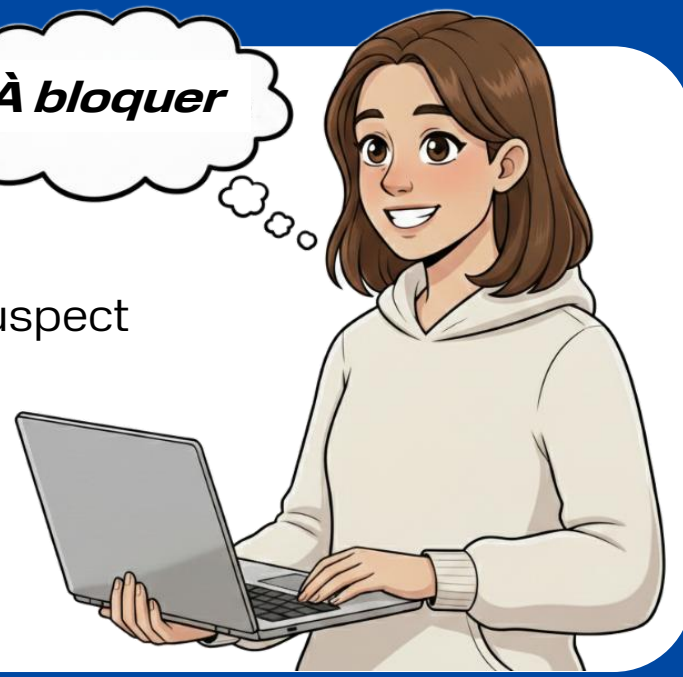
Retenez l'essentiel :

- **Le Dropping** ce n'est pas de l' « argent facile », mais un **crime passible de sanctions pénales**
- **La responsabilité incombe** aussi bien aux organisateurs qu'aux **participants ordinaires**

Règles de sécurité

Si vous détectez des signes de recrutement :

- Cessez tout contact avec les fraudeurs
- N'effectuez aucun transfert, même si vous avez reçu un virement suspect
- Bloquez votre carte et informez votre banque
- Conservez les échanges, coordonnées et numéros des fraudeurs
- Contactez les forces de l'ordre



Toute offre « d'argent facile » est suspecte

surtout si elle exige des données personnelles ou l'accès à vos cartes bancaires

Histoire et caractéristiques

Qu'est-ce que la cryptomonnaie :

- Monnaie numérique indépendante des banques d'État
- Fonctionne sur la blockchain — un registre décentralisé de transactions

3 janvier 2009

Génération du premier bloc Bitcoin

Croissance phénoménale de la valeur

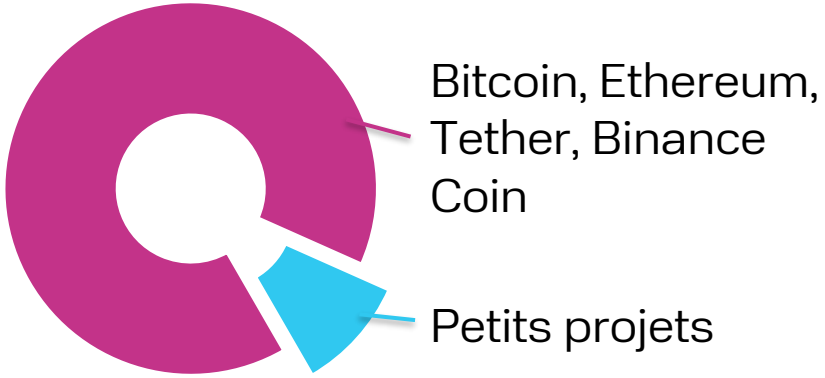
2009 **1 cent**

2025 **$126 200**

Rentabilité passée ≠ rentabilité future

Principaux crypto-actifs

en 2026



Rouble numérique vs Cryptomonnaie

Rouble numérique

- Complète les espèces et les fonds non liquides
- Contrôlé par la Banque de Russie, accessible via applications mobiles et internet-banque
- Procédure KYC obligatoire pour lutter contre la fraude et le blanchiment d'argent

Actif d'État et contrôlé

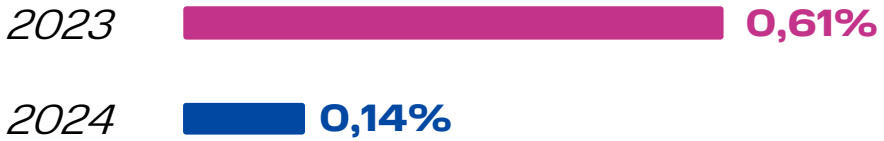
Cryptomonnaie

- Utilisée comme actif / bien, pas toujours un moyen de paiement légal
- Décentralisée — aucun contrôle unique des États ou des banques
- Pseudonyme : liée à l'adresse publique du portefeuille, risques de sécurité

Actif décentralisé à forte volatilité

Cryptomonnaie et fraude

Part des transactions criminelles



Entités présentant des signes d'activité illégale

Statistiques de la Banque de Russie

3346
janv.–juin 2024

4183
janv.–juin 2025

Utilisation par les criminels

- Drogues, jeux d'argent, vol de propriété intellectuelle
- Blanchiment d'argent, pyramides financières
- Les cryptomonnaies — un moyen d'attirer des fonds et des investissements avec promesse de gains rapides

La cryptomonnaie est prisée des jeunes,

mais constitue un outil de fraude, particulièrement avec l'IA pour toucher un large public

Le triangle frauduleux P2P

Comment fonctionne le schéma

Fausse annonce

Vente d'un article à un prix inférieur au marché

→

Substitution des coordonnées bancaires

Carte du trader P2P, et non celle du vendeur

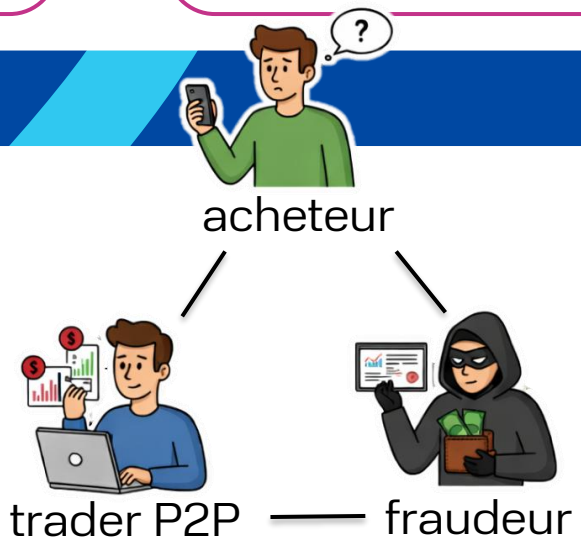
→

Virement des fonds au trader P2P

Achat de cryptomonnaie pour les fraudeurs

Comment réduire les risques

- Vérifier les évaluations et l'historique des contreparties
- Choisir des modes de paiement courants et traçables
- Vendre des articles uniquement sur des plateformes de confiance



L'arnaque de la cryptomonnaie SQUID

Ce qui s'est passé

- Le jeton Squid devait être utilisé dans un jeu en ligne basé sur une série populaire
- **En 2 jours, flambée de 44 000 %,** prix **de 2 860 $**
- Peu après, effondrement à 0
- **Les fraudeurs ont détourné >3 millions $,**
- plus de 40 000 investisseurs victimes

Signaux d'alarme

- Impossibilité de vendre le jeton
- Absence de cotation sur les bourses connues

Important

- Avant d'investir, vérifier les créateurs du projet et les informations disponibles
- Prudence et esprit critique = protection contre la fraude financière

La pyramide Bitconnect

Principe du schéma

- **Déguisement** en plateforme crypto avec IA pour le trading
- Promesse de rendements élevés avec un minimum de risques
- **Programme** de parrainage : 7–15 % des dépôts des nouveaux participants

Conséquences

- Investisseurs de plus de **40 pays victimes**
- Pertes s'élevant à **> 17 millions $**

Mécanisme de la tromperie

- L'argent des nouveaux investisseurs → paiement des « bénéfices » aux anciens et bonus → poches des organisateurs
- Le robot de trading n'existait pas

Garanties de rendements élevés
+
bonus de parrainage
=
signal clair d'une arnaque financière

Pyramide financière Finiko

Principe du schéma

- Éliminer ses dettes grâce aux investissements
- Utiliser des «modèles mathématiques» et l'IA pour «réduire les risques»
- Possibilité d'acheter un appartement ou une voiture à 35 % du prix
- Dépôts avec un rendement de 20 à 30 % par mois

Mécanisme de la tromperie

- Toutes les transactions effectuées en Bitcoin et Tether.
- Dépôts en monnaie fiduciaire interdits.
- Popularité du système a augmenté grâce à des offres très lucratives.

Revenus élevés + incapacité à utiliser l'argent courant = signe évident de fraude

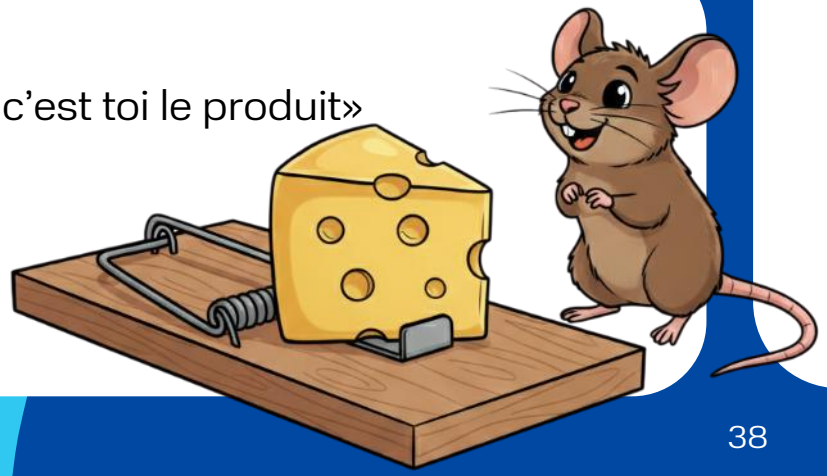
Règles de sécurité

Vérifiez la légalité

- Tous les établissements financiers doivent être agréés par la Banque centrale de la Fédération de Russie.
- Consultez le répertoire : *cbr.ru/inside/warning-list*

Règle de base-

«Si c'est gratuit- c'est toi le produit»



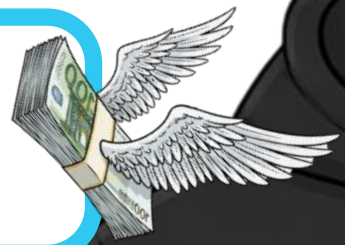
A quoi identifie-t-on une pyramide financière

- Promesses irréalistes de rendements plusieurs fois supérieurs au marché
- Programme de parrainage
- Absence de licence et de documents
- Publicité agressive et une urgence extrême (« pas plus tard qu'aujourd'hui! »)
- Manque de transparence : aucune information sur l'équipe de la direction ou l'enregistrement légal
- Acceptation de l'argent liquide ou de cryptomonnaies sans justificatif

Objectif principal des arnaqueurs

Réduire la vigilance et bloquer l’esprit critique de la victime

Les schémas changent,
la nature de l’arnaque persiste



Boutiques et sites web d'hameçonnage

Schémas des arnaqueurs

Les fraudeurs créent des copies des sites web de magasins, de compagnies aériennes, de banques, etc.

→ Ils proposent des produits divers, des billets et des forfaits de voyage à prix réduit, attirant ainsi la victime.

Règles de sécurité

Faites vos achats uniquement via les applications officielles

Evitez de suivre les liens proposés dans les courriels

Vérifiez bien que c'est un site **https**, et non pas http

Procurez-vous une carte bancaire à part pour les achats en ligne

Vérifiez s'il n'y a pas de fautes dans le nom du site

Installez un logitiel antivirus

Livraison des fleurs avec «Gosuslugi»

Mécanisme de l'arnaque

Un appel du «service de livraison»

pour confirmer l'achat il faut dire le code reçu dans un SMS

→

Un appel depuis «Roskomnadzor»

qui vous signale un état d'alerte

→

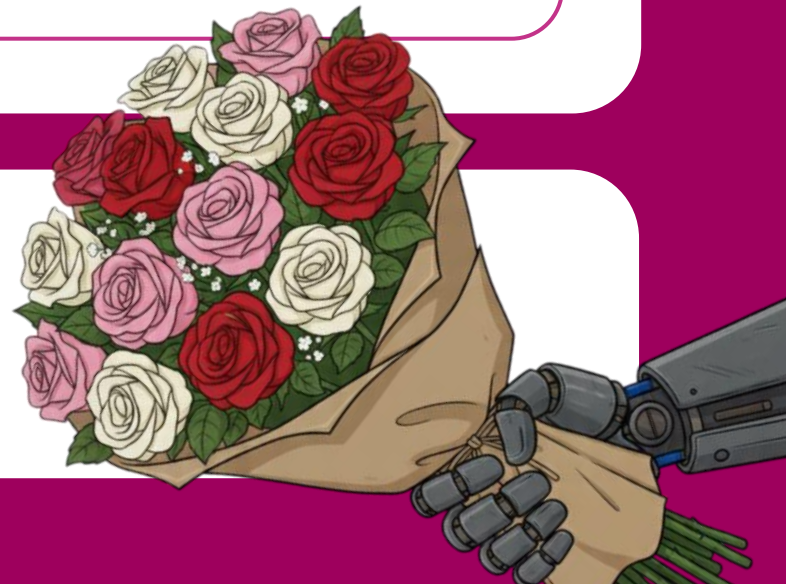
Deuxième appel du «service de sécurité»

pour vous aider à réinitier l'accès à «**Gosuslugi**»

Règles de sécurité

- Ne jamais communiquer les codes reçus par SMS – ce sont des codes
- pour microcrédits!
- Posez-vous la question: cette livraison est-ce bien pour moi?

Si vous n'avez rien commmandé- c'est de l'arnaque



Bloquer les cartes à l’aide de l’IA

Mécanisme de l’arnaque

Ils appellent la banque en se faisant passer pour un «client»

Ils communiquent vos données personnelles, imitent votre voix

→

La carte est bloquée

Raisons: une perte, un vol et autres

→

La victime reçoit des menaces

On demande de l’argent à la victime

Règles de sécurité

Si vous appelez la banque, faites le bon numéro qu’on trouve sur le site officiel

En aucun cas ne faites par de transfert d’argent

Discutez en famille de la situation qui vous arrive

Problème global

Population adulte du monde

57%
ont connu des cas d'arnaque

54%
ont été arnaqués lors des achats en ligne

48%
sont victimes des investissements fraudés

Suite psychologique

69%
sont beaucoup stressés

14%
ont des relations familiales qui se dégradent

17%
ont de moins en moins de confiance en soi

L'esprit critique et la bonne maîtrise du numérique c'est le rempart le plus fort.

- Près d'une personne sur quatre, même parmi celles qui se considèrent prudentes, continue à perdre de l'argent.
- Les escrocs perfectionnent sans cesse leurs techniques, et la simple vigilance ne suffit plus.

Sécurité financière
Olympiade internationale

Les activités à accomplir dans le cadre de l'Olympiade ont pour point de départ les matières suivantes:

Elèves des écoles

- maths
- informatique
- science sociale

Etudiants

- Relations internationales, études régionales
- Économie, finances, sécurité économique
- Mathématiques, sécurité de l'information
- Jurisprudence

Prix et privilèges

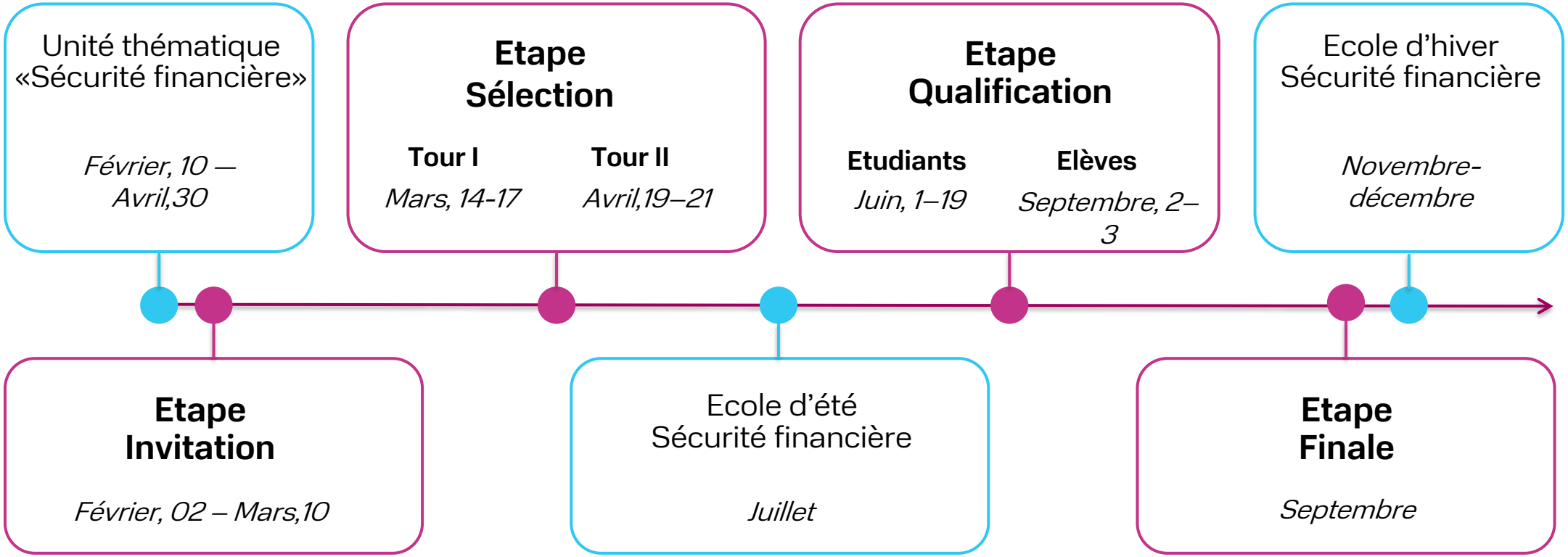
✓ **Réductions sur les frais d'inscription dans les universités membres de l'Institut** virtuel international (Licence, Master, Doctorat)

✓ **Possibilité de faire un stage à** Rosfinmonitoring et dans d'autres entreprises

rosfinolymp.ru

Sécurité financière
Olympiade internationale

sodrujestvo.org



Partenaires

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ФИНАНСОВОМУ МОНИТОРИНГУ

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

РУДН

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МУМЦУМ

содружество

ПСБ

ЦЕНТР МЕЖОЛИМПИАДНОЙ ПОДГОТОВКИ