Principales lignes de défense contre la fraude à l'identité synthétique : usurpation d'identité et prise de contrôle de compte

Évolution de l'état de la menace

Entrée en relation avec les clients : usurpation d'identité et fraude à l'identité synthétique

- L'usurpation d'identité se sert de données à caractère personnel (DCP) et de documents volés, mais authentiques, pour usurper l'identité de personnes réelles.
- La fraude à l'identité synthétique mélange délibérément des éléments réels et d'autres inventés de toutes pièces pour créer des identités fictives évolutives, composées de données d'identité plausibles et cohérentes.
- Les identités synthétiques passent souvent avec succès les contrôles préalables à toute entrée en relation avec le client, car le fraudeur crée l'identité, l'historique auquel il est relié et les pièces justificatives de A à Z.
- L'absence de victime clairement identifiée retarde le signalement et donne aux fraudeurs le temps de se constituer une certaine légitimité.

Une fois le compte ouvert : prise de contrôle du compte (Account takeover ou ATO)

- Les fraudeurs compromettent les données d'identification par le biais de l'hameçonnage, d'échanges de cartes SIM, de techniques d'interception ou en jouant le rôle d'intermédiaire « ou man-in-the-middle ».
- Les mots de passe à usage unique et les facteurs d'authentification statiques sont de plus en plus inefficaces lorsqu'ils sont utilisés seuls.
- L'intelligence artificielle (IA) permet l'automatisation, la flexibilité et la fiabilité à tous les niveaux.

Usurpation d'identité basée sur l'IA (sur l'ensemble du cycle de vie de la relation client)

- Les deepfakes permettent de créer des identités synthétiques ou artificielles à grande échelle et de les mettre au service de la fraude.
- Des visages contrefaits, le clonage de voix et les attaques par injection (de codes informatiques) peuvent tromper les contrôles en mimant la présence d'une personne et les systèmes de vérification d'identité en ligne.
- Les cyberattaquants combinent de plus en plus la génération de contenus par IA, le détournement d'appareils et le recours au mimétisme de comportements pour échapper aux contrôles.

Pourquoi les contrôles traditionnels échouent-ils ?

- Les documents et les données à caractère personnel (DCP) ne peuvent plus être considérés comme des sources d'informations fiables :
    - Les identités volées sont adossées à des pièces justificatives et des données authentiques.
    - Les fraudeurs peuvent générer ou obtenir des documents très convaincants pour justifier des identités synthétiques.
- Les vérifications ponctuelles ne permettent pas de détecter les anomalies entre plusieurs sessions ou plusieurs canaux.
- Les contrôles basés sur les mots de passe à usage unique dépendent de l'éventuel détournement de cartes SIM, de logiciels malveillants et d'attaques par relais.
- Les méthodes d'authentification classiques n'ont pas été conçues pour détecter l'injection assistée par IA ou l'usurpation d'identité en temps réel.

S’assurer de l’identité des personnes en continu

- Rendre la vie des fraudeurs plus difficile et envisager des contrôles à partir de plusieurs angles et en temps réel.
- Évaluer le risque et distinguer la fraude à l’identité synthétique, le vol d’identité et la fraude par prise de contrôle de compte à l’aide de modèles dédiés.
- Passer d’une vérification statique à une authentification adaptative basée sur les risques tout au long du cycle de vie de la relation client.

Matrice des menaces : Détection et atténuation des fraudes émergentes à l’identité

Menace de fraude	Signaux d’alerte	Détection	Réduction du risque
Fraude à l’identité synthétique	Données à caractère personnel (DCP) cohérentes, mais artificielles, historique de fichiers très limité, mécanismes impliquant le recyclage d’identités.	Vérifications de documents assistées par IA, cartographie des appareils et des identités, signaux de consortiums.	Analyse du réseau, liens inter-institutions, entrée en relation sur la base de l’approche par les risques.
Usurpation d’identité	Vrais documents mais comportements ou appareils en dissonance avec ces documents.	Contrôles biométriques et de présence réelle du client contredisant des informations provenant des appareils, ou des comportements.	Authentification renforcée, re-vérification biométrique, surveillance continue.
Piratage de compte	Changement de comportement, adoption d’un nouvel appareil ou d’une nouvelle adresse IP, anomalies apparues durant la session.	Biométrie comportementale, notation des risques de session.	Contrôles adaptatifs, intervention en temps réel, contrôles au niveau des transactions.

Principes de conception et meilleures pratiques

- **Améliorer la prévention des risques :** détecter les tentatives de deepfake et d’injection au moment de l’entrée en relation avec le client, et non *après* la constatation des pertes.
- **Adaptatif par défaut :** faire remonter les contrôles de manière dynamique en fonction du comportement, de l’appareil et du contexte.
- **Correctifs en continu :** réauthentifier continuellement les utilisateurs en fonction de la biométrie comportementale durant les activités à haut risque.
- **Explicabilité :** contribuer aux enquêtes et aux contrôles réglementaires.
- **Partage d’informations :** utiliser les flux de consortiums et de cyber-renseignements pour identifier les tactiques, techniques et mécanismes émergents des fraudeurs.
- **Test de résilience :** mener régulièrement des tests d’intrusion de type « Red Team » pour faire face aux attaques basées sur l’IA.

Appel à l’action

- L’identité peut être fabriquée de toutes pièces et rester convaincante. Par conséquent, les contrôles doivent être conçus en prenant en compte cet état de fait.
- Ne plus considérer les pièces justificatives et les mots de passe à usage unique comme dignes de confiance absolue.
- Superposer les couches de détection sur l’ensemble des éléments en jeu: signaux générés par les artefacts, le comportement, les appareils et le réseau.
- Tester continuellement ses défenses à l’aune des outils deepfake émergents.

Autres lectures

- **IC3 PSA (FBI) : Fraude à l’identité synthétique ;**
- **Bulletin de renseignement DHS/HSI sur les réseaux de fraude ;**
- **Démasquer la cybercriminalité : renforcement de la vérification de l’identité numérique contre les deepfakes**