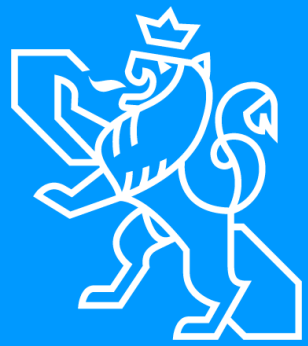
POLICE
LËTZEBUERG

La prévention des fraudes ciblant les personnes âgées



ZESUMME FIR IECH

Généralités

- Limites de la répression
  - Risque d'impunité des auteurs qui agissent sous la couverture protectrice de l'Internet
  - Très faibles chances de recouvrement des avoirs détournés
- Importance de la prévention
  - Effort collectif
  - Effort répétitif
  - Effort évolutif

Généralités

- Le terme « escroquerie » regroupe une panoplie de modes opératoires différents, variables et évolutifs qui traduisent une grande imagination dans le chef des fraudeurs
- Les modes opératoires ciblant entre autres les personnes âgées
  - Arnaques au téléphone
  - Arnaques à la porte d'entrée
  - Arnaques sur Internet – attaques de phishing
  - Autres arnaques sur Internet

Arnaques au téléphone – Les appels choc

- Prise de contact via téléphone
- Pression psychologique sur la victime qui doit payer en urgence une somme d'argent ou alternativement remettre des bijoux pour aider un proche ou se protéger contre des criminels
- Scénarios : 1) un proche est arrêté par la Police suite à un accident mortel, 2) un proche a besoin de soins médicaux urgents suite à un accident, 3) la victime doit se protéger contre des cambrioleurs actifs sur le secteur etc.
- Apparence d'autorité : le fraudeur dit être un policier ou un procureur
- Demande de confidentialité : le fraudeur exige de la victime de ne parler à personne
- Préjudice important

Arnaques au téléphone – Le nouveau GSM du fils / de la fille

- Prise de contact via SMS
- La victime reçoit un SMS d'un numéro inconnu. Dans ce message, le fraudeur se fait passer comme l'enfant de la victime qui utilise un nouveau numéro suite au vol ou la perte de son ancien GSM. L'enfant présumé demande l'aide de la victime pour payer en son nom une facture de plusieurs milliers d'euros au prétexte qu'il n'a plus accès à ses services bancaires en ligne.
- Virements effectués en urgence sur des comptes luxembourgeois ou étrangers.

Arnaques à la porte d'entrée – Le colportage frauduleux

- Offres de services de nettoyage ou de réparation (entrée, toiture, façade) non sollicitées par la victime
- Publicité laissant présumer une entreprise légitime
- Absence de devis écrit ou devis de fortune établi sur place
- Découverte d'autres « dégâts » au cours des travaux pour gonfler le prix
- Qualité médiocre de la prestation
- Mise sous pression de la victime pour être rémunéré
- Autres manœuvres frauduleux (refuser cash pour obtenir carte de crédit de la victime, demander d'entrer dans la maison pour aller aux toilettes…)

Arnaques à la porte d’entrée – Arnaques à la fausse qualité

- Utilisation d’une fausse qualité (policier, agent communal) pour accéder au domicile de la victime
- Finalité est d’entrer dans la maison afin de voler ou de se faire remettre de l’argent ou d’autres objets de valeur

Attaques de phishing

- Mail/SMS contenant un lien dirigeant la victime vers un site falsifié ressemblant à des sites officiels
- Alternative : Appel direct par téléphone
- Mise sous pression en invoquant un quelconque prétexte d'urgence (suspension du compte, mise à jour des données, panne technique, enquête)
- Finalité 1 : récupérer les données personnelles (n° d'utilisateur, mot de passe, n° du compte/de la carte de crédit) de la victime
- Finalité 2 : utiliser les données détournées pour détourner votre argent (virements / retraits)

Autres arnaques sur Internet

- Investment Scam (1)
- Romance Scam (2)
  - Prise de contact par le fraudeur via une application de rencontre ou via les réseaux sociaux classiques
  - Etablissement d'une relation de confiance afin de vous convaincre d'investir de larges sommes d'argent dans des opportunités d'investissement fictives (1)
  - Etablissement d'une relation romantique amoureuse afin de vous convaincre de payer des larges sommes d'argent pour aider financièrement l'amant(e) fictif(ve) ou pour rendre possible le voyage de l'amant(e) fictif(ve) au Luxembourg (2)

Victime d’une escroquerie – quelle réaction ?

Si vous êtes devenu victime

- Informer immédiatement votre banque (compte) ou Worldline (carte de crédit) – importance d’une réaction rapide afin de bloquer les transferts d’argent, sinon risque élevé de perdre tout votre argent.

- Déposer plainte auprès de la Police – pièces à l’appui : extraits de comptes, extraits de la carte de crédit, copie d’écran du message « phishing ».