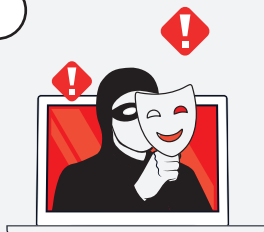


# ATTENTION AU PHISHING PAR SMS, COURRIEL OU TÉLÉPHONE !

1



**L'escroc se fait passer pour un tiers de confiance** (entité étatique, banque...) et vous envoie un lien par SMS ou email. Il peut même téléphoner avec un **faux numéro luxembourgeois**.

2



**Le message** reçu est **alarmant** (p.ex. prélèvements bancaires illicites) **ou attrayant** (remboursement d'impôts, paiement de primes...) et vous incite à **cliquer sur un lien**.

3



Ce lien mène vers un **site web frauduleux**, avec pour finalité de **recupérer vos données personnelles**.

## Conseils préventifs :

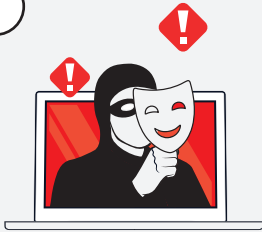
- **Ne partagez jamais des données personnelles avec des inconnus**, ou qui vous sont demandées par courriel, téléphone, SMS ou d'autres services de messagerie.
- **Ne cliquez jamais sur un lien** qui vous a été envoyé d'une **source inconnue**.
- Méfiez-vous de messages ou appels qui vous poussent à réagir vite. **Ne vous laissez jamais mettre sous pression** pour effectuer un paiement ou transmettre vos données, et prenez toujours le temps de remettre en question de telles sollicitations.
- **Contrôlez toujours si le message s'adresse à vous personnellement**, respectivement, s'il contient des **fautes** ou des **traductions erronées**.
- Sachez que des organisations et entreprises sérieuses ne vous demandent jamais d'envoyer des données personnelles via courriel ou SMS.

**Si la provenance d'un message ou d'un appel n'est pas claire, et/ou en cas de doute, prenez d'abord contact avec l'entité concernée par le biais des moyens de communication habituels pour vérifier s'il s'agit d'une arnaque ou pas.**

**Si vous avez été victime d'une escroquerie, contactez l'un de nos commissariats de police pour porter plainte.**

# VORSICHT VOR PHISHING PER SMS, E-MAIL ODER TELEFON!

1



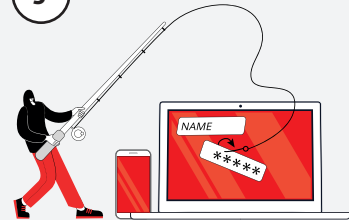
**Der Betrüger gibt sich als vertrauenswürdiger Dritter** (staatliche Behörde, Bank...) aus und sendet Ihnen einen Link per SMS oder E-Mail. Er kann sogar mit einer **gefälschten luxemburgischen Nummer** anrufen.

2



**Die erhaltene Nachricht ist besorgniserregend** (z. B. illegale Bankabhebungen) **oder attraktiv** (Steuerrückerstattung, Auszahlung von Prämien...) und fordert zum **Klicken auf einen Link** auf.

3



Dieser Link führt zu einer **betrügerischen Website** mit dem Ziel, **Ihre persönlichen Daten zu stehlen**.

## Ratschläge zur Vorbeugung:

- **Geben Sie niemals Informationen und persönliche Daten an Fremde weiter**, oder nach denen Sie per E-Mail, SMS oder anderen Nachrichtendiensten gefragt werden.
- **Klicken Sie nie auf einen Link**, der Ihnen von einer **unbekannten Quelle** geschickt wurde.
- Seien Sie misstrauisch bei Nachrichten oder Anrufen, die Sie zu einer schnellen Reaktion auffordern.
- **Lassen Sie sich niemals zu einer Zahlung oder zur Übermittlung Ihrer Daten drängen**, und nehmen Sie sich stets die Zeit, solche Anfragen zu hinterfragen.
- **Prüfen Sie immer, ob die Nachricht persönlich an Sie gerichtet ist**, bzw. ob sie **Fehler** oder **falsche Übersetzungen** enthält.
- Seien Sie sich bewusst, dass seriöse Organisationen und Unternehmen Sie niemals dazu auffordern, persönliche Daten per E-Mail zu senden.

**Wenn die Herkunft einer Nachricht oder eines Anrufs unklar ist und/oder Zweifel bestehen, wenden Sie sich zunächst über die üblichen Kommunikationsmittel an das betreffende Unternehmen, um zu überprüfen, ob es sich um einen Betrug handelt oder nicht.**

**Wenn Sie Opfer eines Betrugs geworden sind, wenden Sie sich an eine unserer Polizeidienststellen, um Anzeige zu erstatten.**