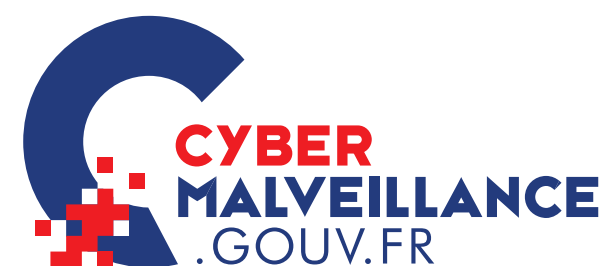




RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité



Assistance et prévention
en cybersécurité



LES ESSENTIELS DE LA SÉCURITÉ NUMÉRIQUE DE VOTRE ORGANISATION



HAMEÇONNAGE Récupération frauduleuse d'informations

Réception d'un message (mail, SMS...) ou d'un appel téléphonique inattendu semblant provenir d'une organisation connue et d'apparence officielle qui demande des informations internes et/ou bancaires.



PIRATAGE DE COMPTE

Accès aux données,
services et contacts

Prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne...

COMMENT PROTÉGER SON ORGANISATION

- **Signaler** toute sollicitation imprévue ou inhabituelle à un responsable ou à un collègue
- Être **vigilant** avec les liens et pièces jointes (mails, SMS...)
- **Ne pas communiquer** d'informations sensibles
- Utiliser des **mots de passe** complexes et différents pour chaque compte ou service
- Ne pas utiliser de **matériels personnels** ou de services non validés
- **Sauvegarder** régulièrement ses données
- **Mettre à jour** régulièrement ses systèmes, applications, antivirus



FAUX ORDRE DE VIREMENT

Provoquer un virement illégitime

L'escroquerie au faux ordre de virement (FOVI) désigne un type d'arnaque qui, par tromperie, production de faux, pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié ou un virement prévu vers un compte frauduleux.



RANÇONGICIEL

Blocage des systèmes
et demande de rançon

Les rançongiciels ou « ransomwares » sont des logiciels malveillants (virus) qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant. Par la suite, les cybercriminels réclament aux victimes le paiement d'une rançon pour en obtenir de nouveau l'accès ou la non divulgation des données récupérées.