

667%

de hausse des attaques de **phishing** en mars 2020.

Le **phishing**, c'est quoi ?

C'est une tentative d'**escroquerie** perpétrée par des cyber-criminels via **mail ou sms**, visant à recueillir les **données personnelles et confidentielles** de leurs victimes.

Comment ? En usurpant l'**identité** d'un tiers de confiance.



Ne **jamais communiquer** vos données personnelles.

Ex : Vos coordonnées bancaires pour un virement du gouvernement



Faire attention à l'**identité** de vos correspondants, et vérifier qu'il s'agit d'une personne de confiance.

Ex : Un mail du gouvernement pour télécharger l'attestation de déplacement



Vérifier avec soin l'orthographe des adresses **URL** de sites "officiels".

Ex : le site <https://www.gouvernement.fr/info-coronavirus> remplacé par <http://www.gouuvernement.fr/info-coronavirus>



Etre vigilant face aux **contrefaçons** frauduleuses liées au coronavirus.

Ex : Vente de faux masques de protection, fausses levées de fond pour des vaccins, demandes de dons



Signaler lorsque vous êtes face à un cas de phishing sur **[phishing-initiative.fr](https://www.phishing-initiative.fr)**