LES ARNAQUES PAR INTERNET

Lors de notre Assemblée Départementale, Alain Gay a fait une présentation rapide sur les différentes arnaques sur internet dont tout un chacun peut être victime. En voici la version plus complète annoncée dans AndreInfos n°49

Tout un chacun, même des plus prudents, peut être un jour victime d'une arnaque provoquée par les moyens de communication moderne que ce soit par smartphone, par ordinateur, par courrier et parfois par QR code. Quelques exemples :

1- Par smartphone :

Vous recevez des SMS étranges,

- Une livraison de colis qui ne rentre pas dans la boite à lettres, et on vous demande de choisir un point relais (il faut payer) ou d'appeler un numéro surtaxé (08xx ou autre)
- Une demande de renouvellement carte vitale, avec vos coordonnées y compris bancaires
- Un Sms avec un lien inconnu
- De fausses offres ou des loteries (c'est votre dernière chance de gagner un iPhone,
- Des news qui vous demandent d'accepter les cookies avec des propositions d'abonnement en ligne automatique si vous refusez

→Attitude : Suivez vos colis sur le site où vous avez passé commande
Ne jamais payer quoi que ce soit surtout par carte bancaire
Utilisez le site de la banque ou de la société qui essaye de vous contacter

Vous avez des appels téléphoniques d'un numéro inconnu

- Semblant venir d'un conseiller bancaire, qui vous signale un mouvement d'argent suspect, vous demande d'agir très vite, et vous demande vos codes
- Faisant du démarchage, (panneaux solaires, fournisseurs énergie)
- Avec comme numéro les 6 premiers chiffres du votre (spoofing), avec un risque d'usurpation d'identité d'une entreprise ou banque.

→Attitude : Ne pas répondre, s'il vous connait le correspondant laissera bien un message,
Si vous répondez dire rapidement que vous n'êtes pas intéressé.

Pour les clients Orange, l'application Téléphone d'Orange (icône Orange) signale s'il s'agit d'un démarchage ou d'un indésirable.

2- Par ordinateur :

Les Mails

- Tentatives d'hameçonnage ***(pishing),*** prudence si on vous demande vos données personnelles d'identité ou bancaires
- Vous recevez un mail vous informant qu'un correspondant a laissé un message sur votre boite vocale, ne pas cliquer sur le lien, mais consulter simplement le répondeur sur votre téléphone
- Arnaques aux sentiments, on vous demande d'envoyer de l'argent à l'étranger pour que votre « amoureux » puisse venir vous rejoindre

- Un gros héritage est bloqué à l'étranger et on vous demande une avance qui vous sera remboursée plus tard.
- Les impôts vous rendent de l'argent mais vous demandent vos coordonnées bancaires : ils possèdent déjà vos coordonnées
- Un faux mail d'un site vous propose des offres alléchantes ==> aller voir directement sur le site officiel
- Vous avez été repéré navigant sur les sites pornographiques (même assoanr42 et le Général Rodriguez censé être l'émetteur du mail en ont été victimes)
- Il vous est réclamé une contravention dont vous n'avez aucun souvenir
- Un copain bloqué à l'étranger sans téléphone vous réclame de l'aide par envoi d'argent (cela commence souvent par « reçois tu mon mail ? »)
- Vous êtes informé de la réinitialisation de votre mot de passe en cours …. Déconnectez-vous et reconnectez pour vérifier sauf si c'est vous qui faites la manipulation

→Attitude : Autant que possible ne pas répondre
Ne jamais donner ses coordonnées bancaires
Ne pas transmettre la copie de sa carte d'identité
Si un correspondant fiable vous demande la copie d'un document, apposez un filigrane sur cette copie : vous pouvez utiliser l'application officielle **https://filigrane.beta.gouv.fr/**
Vérifier l'identité de son correspondant (autrement que par mail)

La navigation sur le WEB

Privilégier les sites dont l'adresse commence par https://.
Eviter les sites aux noms de domaine (caractères après le point dans l'adresse) exotiques. Si .fr , .com , .gouv , .net, .info, .eu sont courants, se méfier de .ru (Russie), .by (Biélorussie), .bz (Bélize) , .ci (Côte d'Ivoire), .pk (Pakistan) par exemple .(Consulter sur Internet **« Liste des domaines Internet de premier niveau »).**
Dans le cas des fenêtres surgissantes, parfois même avec une sirène, signalant une infection par virus éteindre immédiatement votre ordinateur en appuyant 30 secondes sur la touche marche/arrêt. Surtout ne pas appeler le numéro qui s'affiche ou pire donner votre numéro de carte bancaire.
→Attitude : Faire les mises à jour de Windows,
Avoir un bon antivirus à jour,
Ne pas cliquer sur un lien dans un mail, mais aller sur le site concerné.
Soyez attentifs à l'orthographe du mail et des adresses parfois une seule lettre diffère dans le nom.
Utilisez des mots de passe différents et complexes. S'interdire absolument : password, 12345, abcd, azerty, prénoms, nom de votre chien, date de naissance ; des logiciels dits « attaque par force brute » permettent de tester des millions de combinaisons. Vous pouvez en tester la solidité à l'adresse **https://ssi.economie.gouv.fr/motdepasse**

Les réseaux sociaux

Si vous utilisez les réseaux sociaux : méfiez-vous des propositions d'inscription pour des gains ou des cadeaux.

Si une personnalité vous propose un placement exceptionnel, si c'est trop beau, c'est suspect.
Pensez à l'utilisation qui pourrait être faite de vos messages, les cambrioleurs peuvent savoir que vous êtes en vacances loin de chez vous !
Attention aux photos des enfants qui pourraient être réutilisées à des fins douteuses.
Si vous regardez une vidéo, vous recevrez sur les écrans suivants de nombreuses vidéos sur le même sujet.

Comment reconnaître une URL
Une URL est l'adresse d'un site internet exemple : anr42.fr ou www.anr42.fr ou https://www.anr42.fr

Parmi des deux adresses URL 1 = e**-leclerc.communication.fr**

et URL 2 = **communication.e-leclerc.fr**

Laquelle est la bonne ??

C'est la N° 2 ! **communication.e-leclerc.fr**
Où **'e-leclerc.fr'** est le nom de domaine de la société
Et **'communication'** est un sous-domaine

Dans l'URL 1, le pirate a pu acheter le nom de domaine 'communication' et créer un faux sous-domaine 'e-leclerc'
Dans l'URL 2, c'est Leclerc qui est propriétaire du nom de domaine 'e-leclerc' et a créé un sous-domaine 'communication' pour ses besoins officiels de… communication.

3- Par courrier postal :

Vous pouvez recevoir une fausse contravention
Vous avez une information semblant provenir d'un fournisseur habituel (d'électricité par exemple).
→Attitude : bien vérifier les adresses.

4- Par QR code (*quishing*) :

De faux QR Codes sont collés sur des bornes de payement parcmètres ou sur un menu de restaurant. Ils vous renvoient sur un site pirate
→Attitude : Vérifier s'il n'y a pas de double épaisseur.
Ne pas cliquer sur le lien proposé.

Conclusion

La prudence est notre meilleure alliée, n'ayez pas honte, n'hésitez pas en parler autour de vous.
Il ne faut pas céder à la paranoïa mais vous pouvez signaler :

- Les sms frauduleux en envoyant le numéro appelant par SMS au **33700** ou sur le site: **https://www.33700.fr/**
- Les mails frauduleux en envoyant le code source du mail sur le site **https://www.signal-spam.fr/**
- Une cyberattaque sur le site **17Cyber.gouv.fr**

Le site 17Cyber.gouv.fr vous permet éventuellement de porter plainte et contient beaucoup d'infos, n'hésitez pas à le consulter !!

Soyez donc prudents, mais **ne bloquez pas les mails provenant de l'ANR !**

L'ANR42 envoie des mails avec comme expéditeur assoanr42@anr42.fr mais aussi via la plateforme BREVO dont l'adresse de l'expéditeur contient « brevo » ou l'ancien nom « sendinblue ».
L'ANR siège utilise aussi cette plateforme, pour envoyer des infos et des offres de partenaires comme Miléades.
Pour éviter que ceux-ci arrivent en SPAM vous pouvez nous ajouter dans la liste verte (ou de confiance) de votre messagerie.

Alain Gay (assisté par AJM)