Gleizé
Beaujolais

« LA CYBERSÉCURITÉ »
un enjeu majeur

Mairie de Gleizé
04 74 65 37 30
contact@mairie-gleize.fr

www.mairie-gleize.fr

Gleizé ma ville par CITYALL

très Beaujolais

« LA CYBERSÉCURITÉ »
un enjeu majeur

LES MOTIVATIONS DES CYBERCRIMINELS,

dont le profil n'est plus uniquement l'expert en informatique ou *le geek à capuche*, peuvent s'énumérer selon 5 catégories :

1. L'appât du gain
(ransomware ou rançongiciel)

2. Le sabotage
de la part d'un employé licencié mécontent

3. L'accès aux données sensibles
qui peuvent ensuite être revendues
à des tiers ou des commanditaires

4. L'Hacktivisme
comportant une dimension militante politique revendiquée

5. L'espionnage industriel ou étatique
de la part d'une entreprise ou d'un gouvernement

Rappel : *Selon l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), cette menace cybercriminelle a touché particulièrement en 2022 :*

- *Les TPE, PME et ETI (40 % des rançongiciels traités ou rapportés)*
- *Les collectivités territoriales (23 %)*
- *Les établissements publics de santé (10 %)*

On estime de nos jours le coût moyen d'une cyberattaque entre 100 000 et 150 000€.
52 % des entreprises françaises ont subi une cyberattaque en 2022.

LES 10 RECOMMANDATIONS POUR ASSURER SA PROPRE CYBERSÉCURITÉ

1. Protégez vos accès avec des mots de passe solides, suffisamment longs, complexes et différents selon vos équipements et vos usages.

2. Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de celles-là.

3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées.

4. Utilisez un antivirus, vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

5. Téléchargez vos applications uniquement sur les sites officiels (exemples : *App Store, Google Play Store*) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements.

6. Méfiez-vous des messages inattendus ou alarmistes par messagerie (e-mail), SMS ou *chat* et demandez toujours une confirmation à l'émetteur par un autre moyen (*Whats'App, Messenger*, appel téléphonique) si ce message vous semble connu et légitime.

7. Vérifiez les sites sur lesquels vous faites des achats, sinon vous prenez le risque de vous faire dérober votre numéro de carte bancaire, de ne jamais recevoir votre commande ou de recevoir une contrefaçon ou un produit dangereux.

8. Maîtrisez vos réseaux sociaux et évitez la diffusion d'informations personnelles qui ne doivent pas tomber dans de mauvaises mains.

9. Séparez vos usages personnels et professionnels afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise ou organisation, et inversement.

10. Évitez les réseaux WiFi publics ou inconnus (risque de *phishing*).

« LA CYBERSÉCURITÉ »
un enjeu majeur

EN CAS DE CYBERATTAQUE, LES BONS RÉFLEXES À ADOPTER

1 **Déconnectez du réseau tous les ordinateurs infectés** ainsi que les disques externes et autres terminaux reliés.

2 **Contactez des prestataires externes expérimentés en neutralisation des attaques informatiques,** ou votre propre prestataire, qui sauront vous guider dans les premiers instants.

3 **Ne payez pas la rançon demandée et portez plainte** auprès de la police ou la gendarmerie. Des services spécialisés se chargeront ensuite de l'enquête.

Rappel : il est possible de récupérer l'argent ou les données volées dans un délai de 24 h après le début de la cyberattaque, c'est beaucoup moins sûr jusqu'à 48h et au-delà de ce délai d'intervention c'est quasiment impossible.

4 **Avertissez la CNIL dans les 24h** si des données à caractère personnel ont été dérobées.

5 **Prévenez l'ANSSI dans les meilleurs délais,** si vous êtes un opérateur d'importance vitale (établissement hospitalier, SDMIS).

6 **Signalez les faits dont vous êtes victime sur la plateforme de signalement « Pharos »**, afin d'alimenter une meilleure connaissance du phénomène des cyberattaques.

7 **Elaborez un plan de communication pour rassurer vos clients,** vos partenaires ou vos usagers.

NB : En amont d'une cyberattaque, il est utile de sensibiliser vos collaborateurs ou vos agents des bons gestes à effectuer. Il est également conseillé de mettre en place régulièrement de fausses attaques ou des tests visant à acquérir les bons réflexes et à diminuer les effets néfastes du stress ou de la panique, inhérents à une telle situation.

Pour tout renseignement complémentaire sur la cybersécurité :
https://www.cybermalveillance.gouv.fr/
https://www.ssi.gouv.fr/