acf-fgv
association des communes fribourgeoises
freiburger gemeindeverband

Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

VILLARS-SUR-GLÂNE

POLICE

Cybersécurité

Prévenir, soutenir, agir

23.01.2025

Programme

1. Introduction
2. Prévention: *quels bons comportements adopter?*
3. Audits et labellisation: *comment ça marche?*
4. Exemples de communes: *procédure et formation*
5. Comment réagir en cas de suspicion, d'attaque ou de menace?
6. Cyberboîte
7. Conclusion

Sensibilisation à la cybersécurité

Jean-Roland Schuler, jean-roland.schuler@hefr.ch

François Buntschu, francois.buntschu@hefr.ch

Michael Mäder, michael.maeder@hefr.ch

Références

[1]: www.ebas.ch (eBanking but secure, DE, FR, IT, EN)

[2]: www.ibarry.ch (Internet security platform, DE, FR, IT, EN)

[3]: www.ncsc.admin.ch (National Cyber Security Center NCSC, DE, FR, IT, EN)

Plan de la présentation

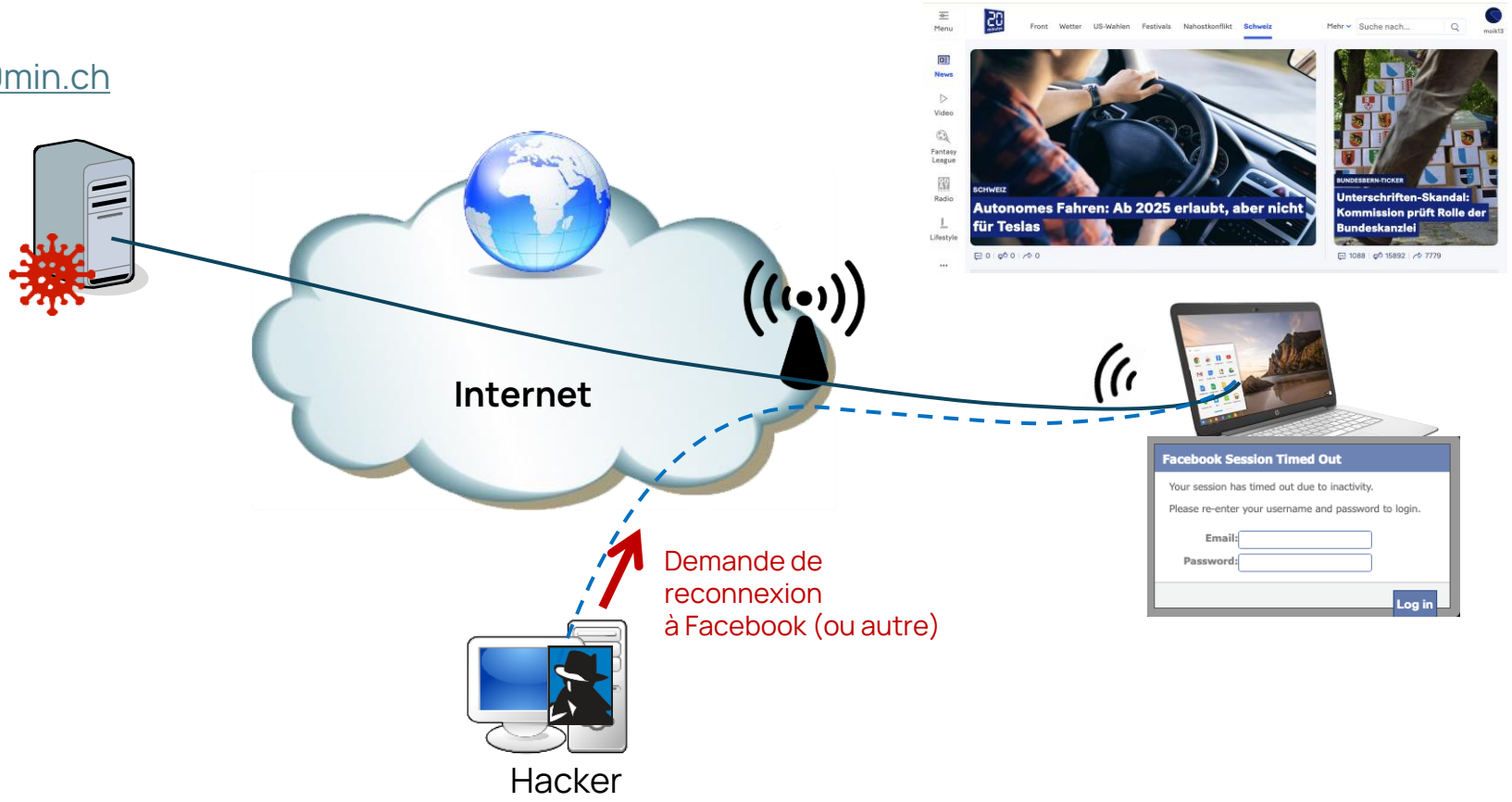
- Démonstrations
- Règles de sécurité
- Que faire en cas de problème
- Virus, ransomware, …, comment on peut être infecté
- Mos de passe
- HTTPS, VPN

Démo - Scénario

- Le site web piraté est la cible vers laquelle une victime doit être dirigée.
- La visite du site web connecte en arrière-plan le navigateur de la victime avec le pirate.
- Le pirate peut faire exécuter différentes actions sur l'ordinateur de la victime (p. ex. demander des informations d'identification).
- Le hacker peut utiliser les credentials obtenus directement ou sur d'autres services.
- Le pirate peut essayer de craquer des mots de passe avec un nom d'utilisateur/email

Démo – Vol de mot de passe

https://20min.ch



Règles pour ordinateur, smartphone, tablette

Règles pour le service informatique

- Avoir un antivirus à jour
- Mises à jour de tous les programmes
- Faire des sauvegardes et être sûr de pouvoir les lire. L'appareil de sauvegarde doit être déconnecté après une sauvegarde
- Bloquer l'écran si pas d'activités

Règles pour la personne

- Utiliser des mots de passe complexes, exemple: *Ifb2j/@aSeVs*. N'utilisez jamais plusieurs fois le même mot de passe
- Fermer ou bloquer les sessions lorsqu'on quitte son poste de travail
- Ne pas utiliser des clés USB inconnues
- Ne pas utiliser des WIFI public sans VPN
- Ne pas utiliser les réseaux sociaux sur les postes professionnels
- Être vigilant, faire preuve de bon sens
- Ne pas donner ses données personnelles

Comment réagir en cas de cyberattaque

Isoler

- Se déconnecter d'Internet (Retirer le câble Ethernet et désactiver le wifi)

Communiquer

- Contactez votre responsable informatique
- Informez vos collègues et l'administration
- Examinez si il faut contacter la police et d'effectuer une dénonciation pénale.
- Attendez que la police ait sauvegardé les traces avant de restaurer les systèmes. Des spécialistes de la police vous conseillent et vous secondent pour savoir comment procéder, sauvegardent les traces et enquêtent. Vous trouvez sur www.suisse-epolice.ch le numéro de téléphone du poste de police le plus proche.

Comment réagir en cas de cyberattaque

Planifier

- Elaborer rapidement et avec attention la réponse à donner à l'incident et les mesure à déployer (protection de données sensibles, reconstruction de systèmes)

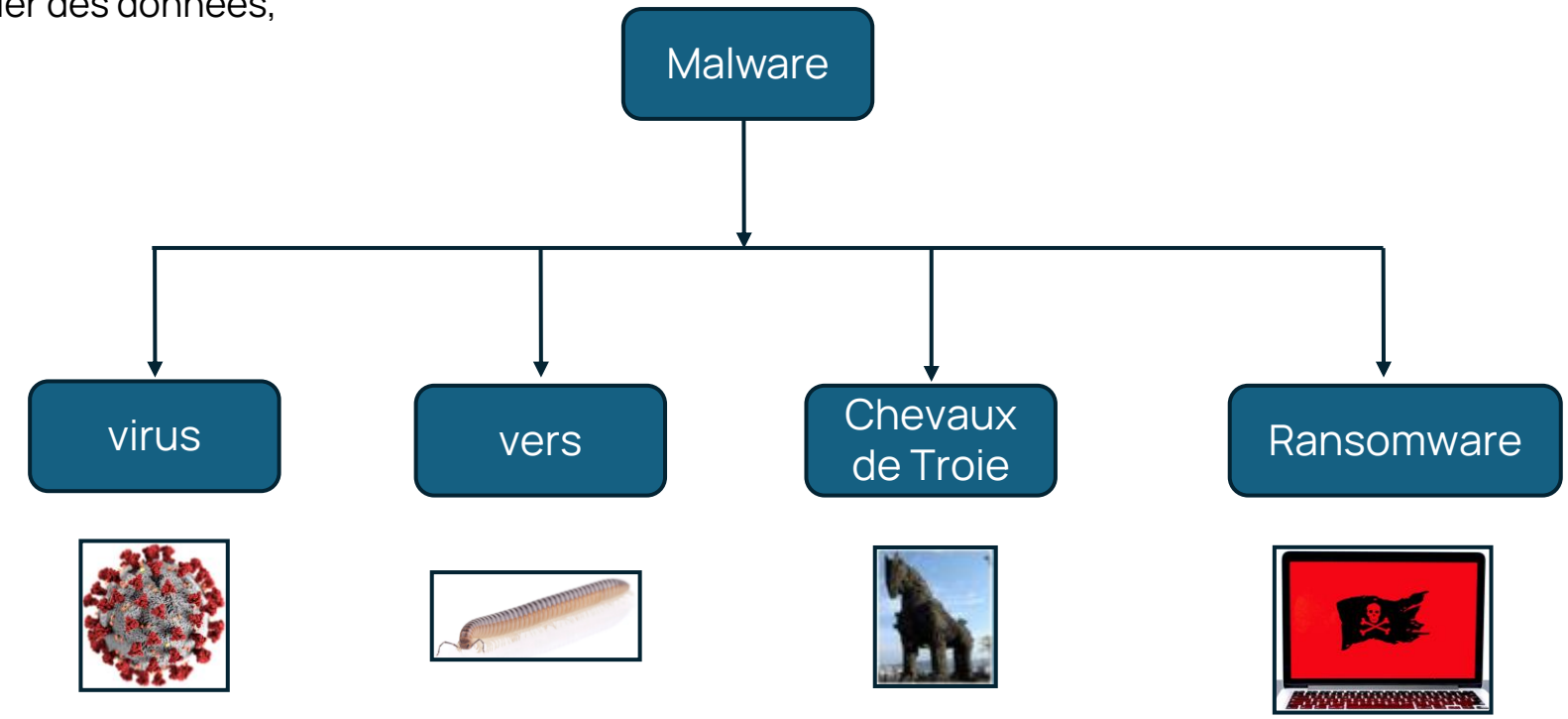
S'en remettre

- Evaluer les mesures à mettre en place pour réduire la probabilité d'un nouvel incident similaire
- Former les collaborateurs

Programmes malveillants (Malware)

- Malware est un terme général qui englobe tous les programmes malveillants comme: les virus, vers, chevaux de Troie, ransomware, …

- Un malware peut: chiffrer, voler, modifier des données, enclencher la caméra, ...

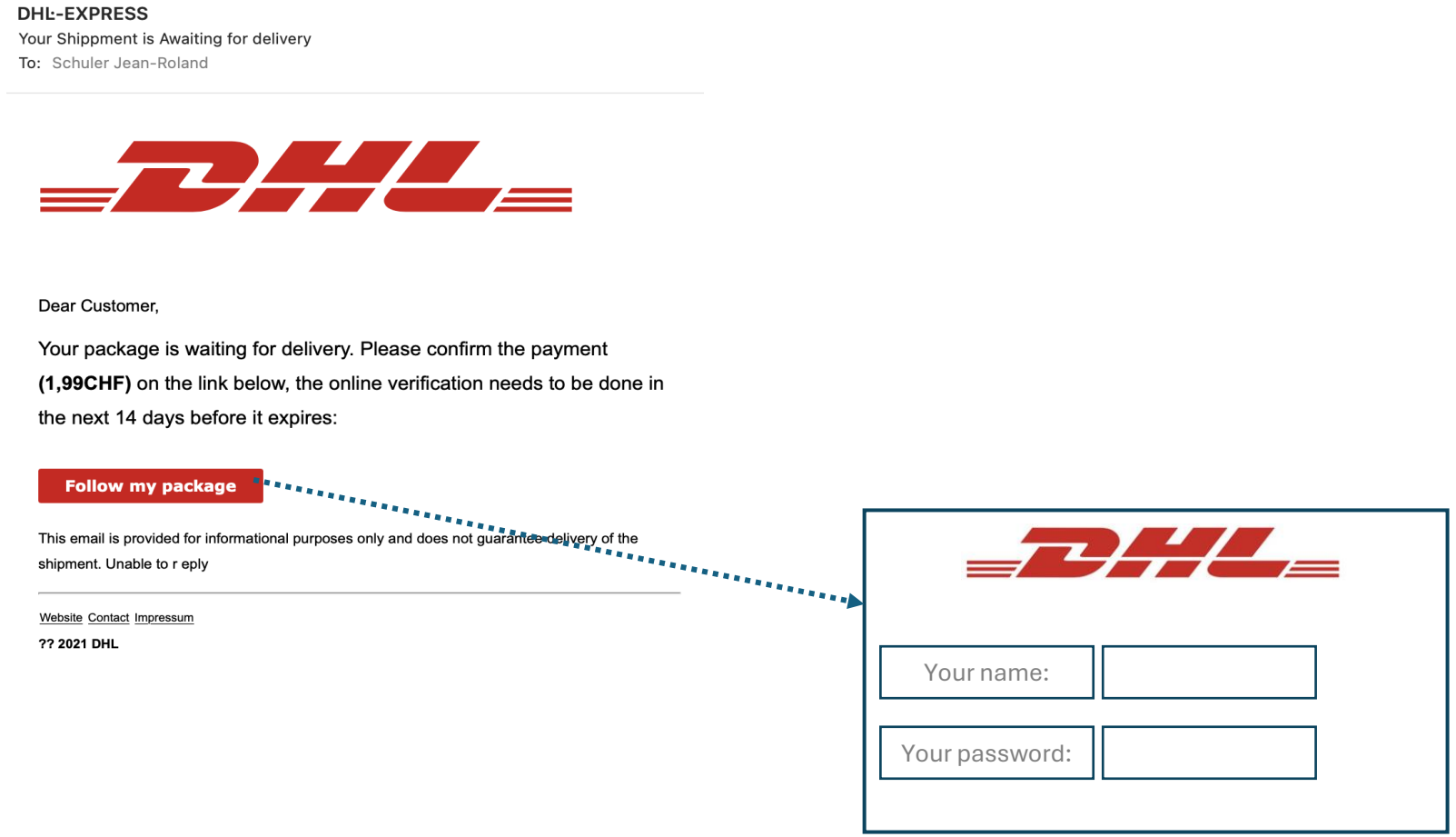


Quelques chiffres [2]

- 500 000 nouveaux malwares détectés par jour
- 50 millions de comptes Facebook compromis
- 91% des cyber attaques commencent avec un e-mail frauduleux pour voler des mots de passe (spear phishing) et ensuite installer un "ransomware"
- Environ 1-2 millions de tests d'attaques par jour sur des sites peu connus
- Les cyber-attaques concernent toutes les entreprises, communes, personnes

Comment mon appareil est-il infecté ?

- Phishing: Pièces jointes et lien dans les e-mails



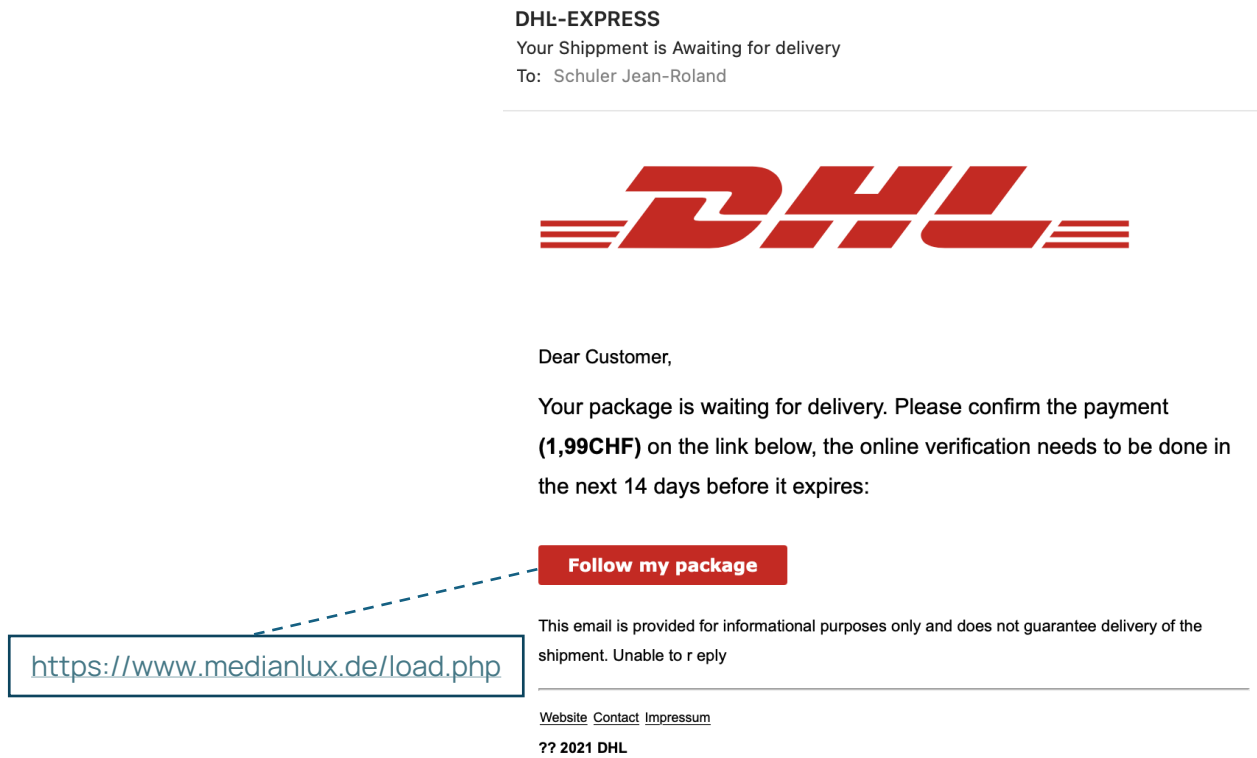
Phishing

- Référence à une société connue
- Annonce d'un problème imminent (Réception d'un paquet, blocage d'un compte)
- Faux e-mail d'une personne

Règles:

- Ne pas cliquer sur l'hyperlien
  Seulement sur PC (pas smartphone, tablette) : si on pose la souris sur l'hyperlien, sans cliquer, on voit la destination)

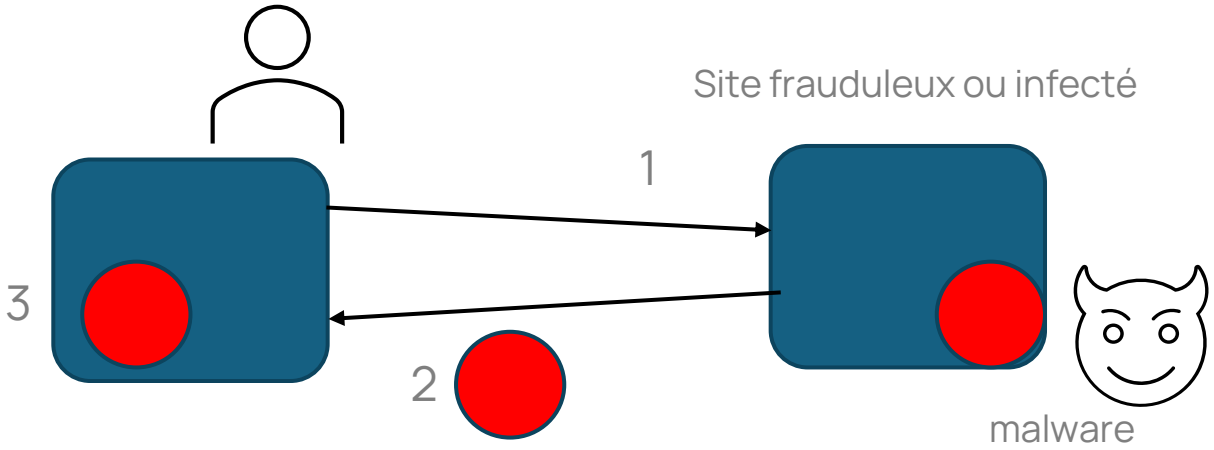
- Réfléchir avant de faire une action



Infection par un malware

Téléchargement d'un site frauduleux ou infecté.

1) l'utilisateur se connecte sur un site qui a été infecté
2) le malware est copié sur l'ordinateur de l'utilisateur
3) le malware fonctionne, il peut:
    - Chiffrer le disque dur
    - Copier les données du disque dur
    - Copier toutes les touches tapées au clavier
    - Enclencher la caméra, le micro
    - ...



Exemple:

le malware Gozi est actif depuis plus de 10 ans.

En 2016, le site 20min.ch a été infecté par Gozi

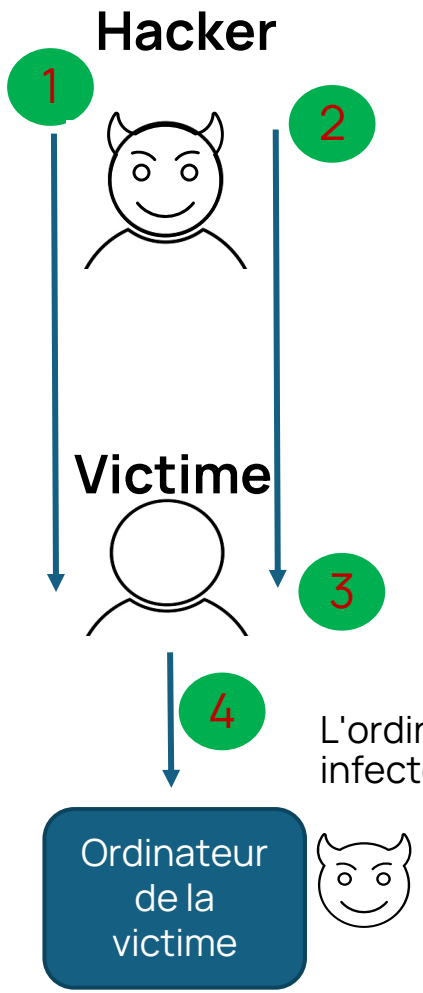
En 2020, une variante de Gozi était envoyée par e-mail avec un fichier attaché.

Protection: Anti-virus et mises à jour

Social engineering et malware [3]

A l'aide des réseaux sociaux, un hacker s'est renseigné sur la victime.

Il téléphone à la victime. Il raconte une histoire et il indique qu'il va envoyer un e-mail avec un fichier attaché



Juste après le téléphone, l'e-mail avec le fichier frauduleux est envoyé

La victime ouvre le fichier

L'ordinateur de la victime est infecté par un malware

Protection:

- Comportement
- Anti-virus
- Mises à jour

Mots de passe

Un bon mot de passe doit avoir:

- Minimum 14 caractères
- Des majuscules, minuscules, chiffres, caractères spéciaux
- Pas de suite de lettres: *asdf1234*
- Pas de "vrais" mots: maison123, voiture$
- Un mot de passe différent par site
- N'utilisez pas ç, é, è, ä, ü, …

Voici un bon mot de passe:

`Ifb2J/a@SeVseS`

- Le problème est de s'en souvenir
- En plus, il faut des mots de passe différents par site: "password manager"

Mots de passe

`Il fait beau 200 jours par an à Sierre en Valais en Suisse`

`Ifb2J/a@SeVseS`

Une autre astuce, utilisez une longue phrase (sans espace):

`En2020-2021ilyaeulap@ndemie`

27 caractères, minuscules, majuscules, chiffres, caractères spéciaux

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

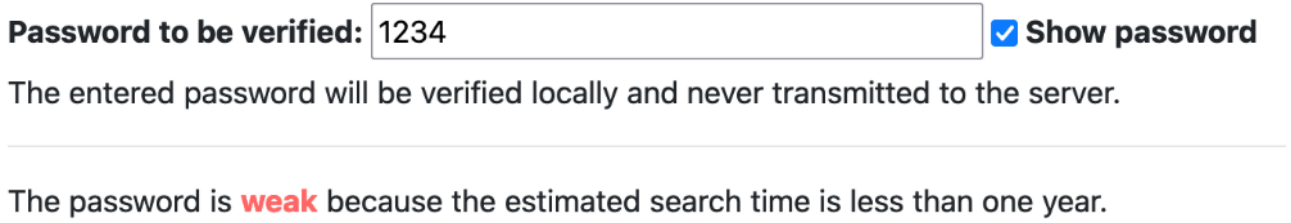
HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

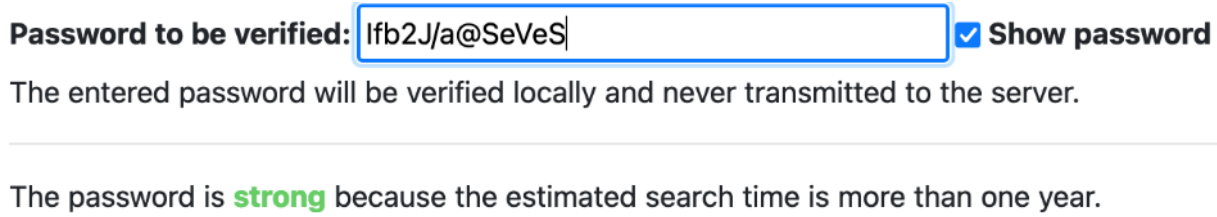
Tester la qualité de votre mot de passe

Vous pouvez tester votre mot de passe (ou un mot de passe similaire) avec ce site: www.passwortcheck.ch

Mot de passe faible:



Mot de passe fort:



Tester si l’adresse email est compromise

Utiliser des outils comme https://haveibeenpwned.com/ pour tester son adresse e-mail

Que faire si votre adresse e-mail se trouve dans "haveibeenpwned"

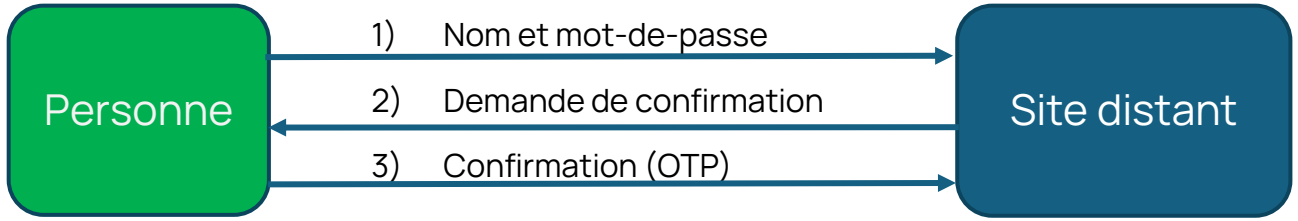
- Changer de mot de passe (attention si vous utilisez 1 seul mot de passe)

Il est possible de s'inscrire chez https://haveibeenpwneed.com afin d'être informé lorsque l'adresse e-mail est dans leur base de données

Authentification à 2 facteurs

Si c'est possible, utilisez une authentification à deux facteurs:

1. Vous indiquez votre nom et mot de passe (Facteur 1)
2. Le site distant demande une confirmation avec un **OTP** (*One Time Password*). La confirmation arrive sur le smartphone (SMS, MobileID, Authenticator, …) ou dans une autre application (p.ex. RSA Token) (Facteur 2)
3. Vous confirmez votre connexion



Un mot de passe par site

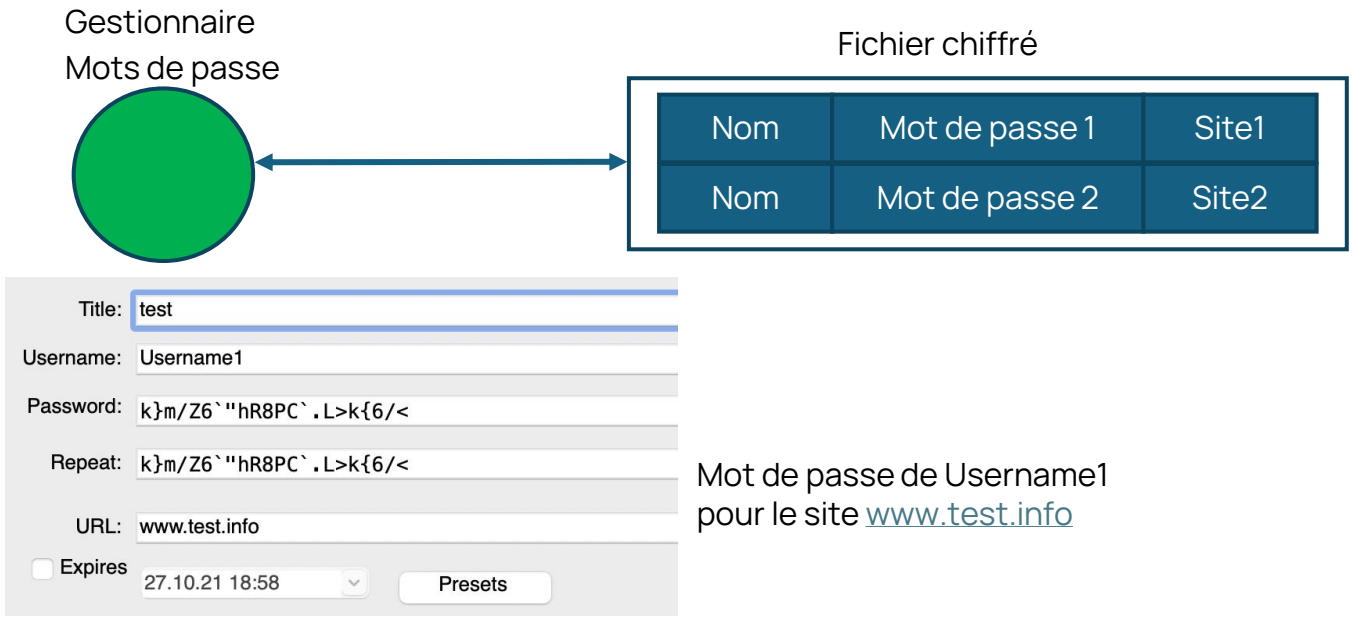
- Souvent les personnes utilisent le même mot de passe partout. Si le mot de passe est volé, les hackers ont accès à tout.

- Il faut avoir un mot de passe différent par site. Pour ceci, utilisez un gestionnaire de mots de passe:
  - NordPass
  - LastPass
  - 1Password
  - KeePass
  - Bitwarden

- Ne **jamais** enregistrer les mots de passe dans le navigateur!
- Ne **jamais** écrire les mots de passe sur un papier (PostIt)

Gestionnaire de mots de passe

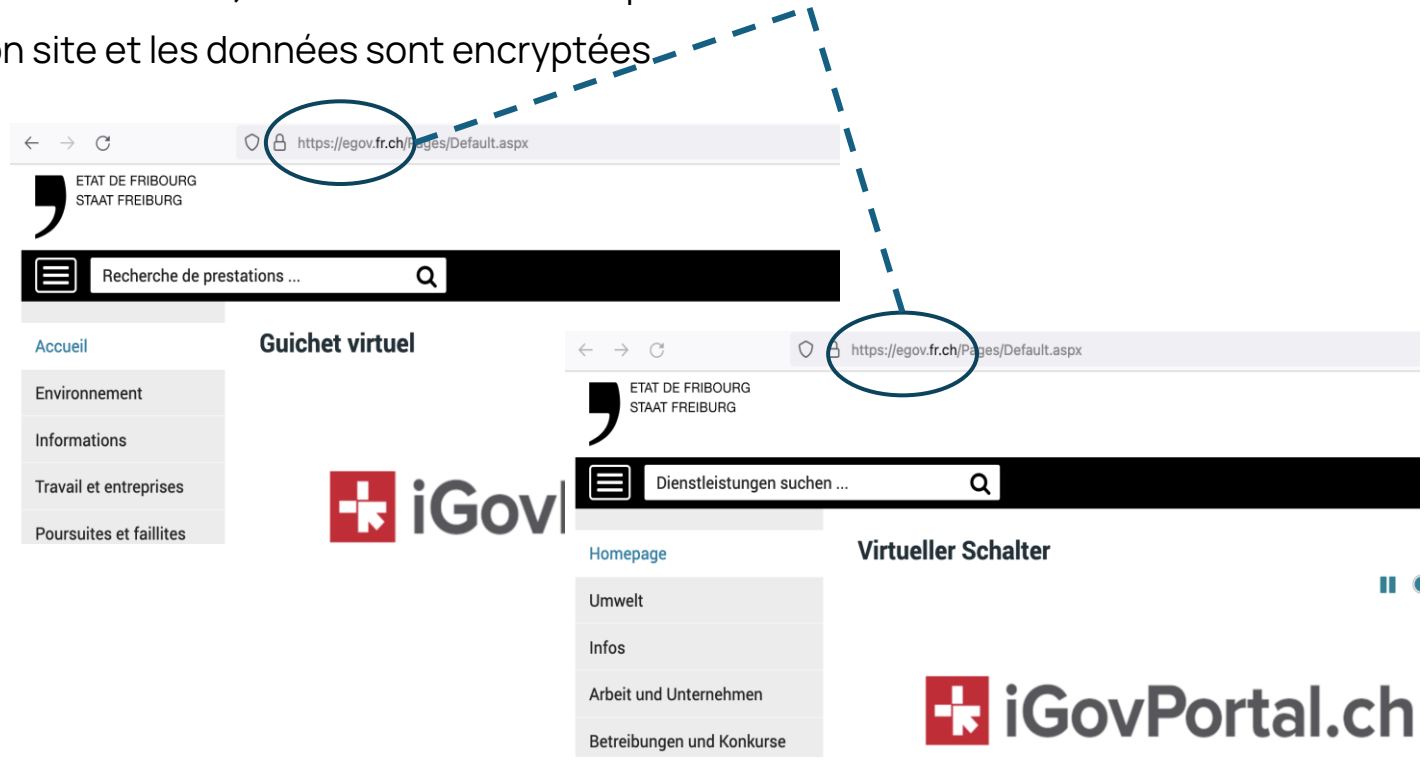
- Un gestionnaire de mots de passe sauve les mots de passe, noms, sites dans un fichier qui est chiffré (encrypté).
- Pour chiffrer et déchiffrer le fichier, l'utilisateur connait un seul mot de passe (qui doit être sûr).



Mot de passe de Username1
pour le site www.test.info

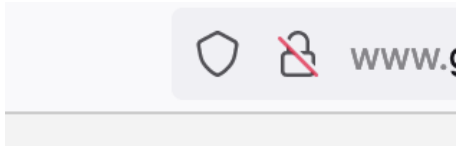
Accès distants sécurisés, https

- Lorsqu'on se connecte vers un site officiel (canton, communes, …), il faut contrôler le https et le cadenas
- https veut dire "sécurisé", on est connecté sur le bon site et les données sont encryptées

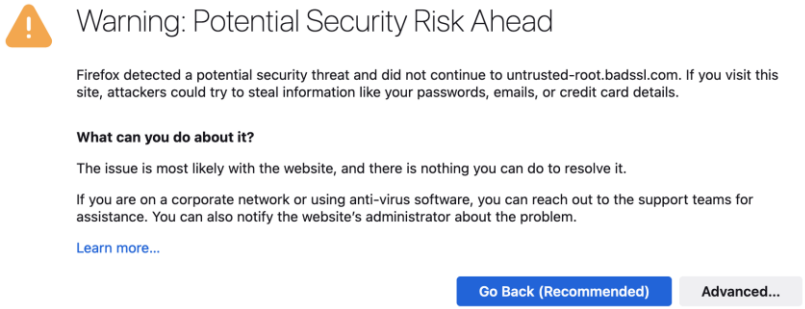


Accès distants sécurisés, https

- Vous êtes connecté sur un site officiel qui n'a pas le https et le cadenas est barré



- Durant la connexion, vous avez eu des messages d'erreurs

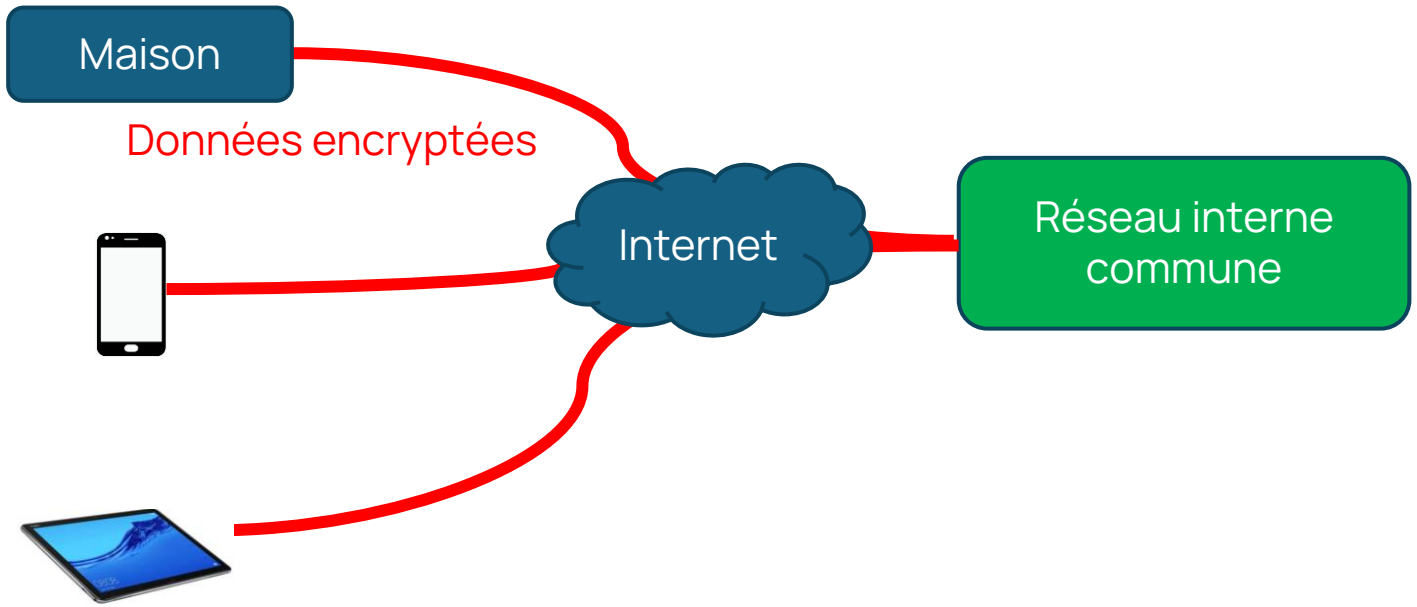


Règle: N'allez pas plus loin et renseignez-vous au service informatique de la commune

Accès distants sécurisés, VPN

- Si vous devez accéder au réseau interne de la commune depuis un ordinateur, un smartphone, une tablette, vous devez utiliser un programme VPN qui sécurise et encrypte les communications

- Ce programme est installé par le service informatique



Boîte à outils

Voici une liste de questions essentielles pour contrôler la sécurité

- Mise à jour de l'OS (Windows, MacOS, Android, iOS)
- Mise à jour des applications habituelles (Word, Excel, **Browser** (!) …)
- Mise à jour des applications propres à la commune (Contrôle habitant, impôts, comptabilité, …)
- Avez-vous un anti-virus et est-ce qu'il est à jour, est-il actif?
- Qualité des mots de passe et leur gestion
- Qui informer en cas d'erreurs (ouverture d'un fichier malveillant, alerte de l'anti-virus, ..)
- Est-ce qu'il y a des sauvegardes, où sont les sauvegardes, est-ce qu'on peut lire les sauvegardes, on sait comment faire?
- Est-ce que la commune à fait un audit de sécurité informatique?

Audits et labellisation: *Comment ça marche?*

Jean-Roland Schuler, jean-roland.schuler@hefr.ch

François Buntschu, francois.buntschu@hefr.ch

Michael Mäder, michael.maeder@hefr.ch

Références

[1]: https://www.srf.ch/news/schweiz/it-sicherheit-von-name-bis-ahv-nummer-sind-die-daten-auf-der-gemeinde-sicher (Von Name bis AHV-Nummer: Sind die Daten auf der Gemeinde sicher?, DE)

[2]: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (Global Security Index 2024 – ITU Publications, International Telecommunication Union (ITU), EN)

[3]: https://www.iso27001security.com/html/iso27000.html (About the ISO27k standards, EN)

[4] https://www.cyber-safe.ch/ (Le label suisse de cybersécurité, DE FR)

Plan de la présentation

- Audits, standards, labels : à quoi ça sert?
- ISO 27k
- CyberSafe, le label suisse
    - CyberSafe, comment ça marche

A quoi sert un audit / label?

- Déterminer la maturité actuelle en termes de cybersécurité
- Mettre en place des améliorations
  - Courte terme
  - Longe terme (processus)
- Sensibilisation des utilisateurs pour la cybersécurité

Exemple du standard ISO27k

About the ISO27k standards

Search

Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | About us

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27009
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016

The "ISO27k" suite comprises more than seventy standards in the ISO/IEC 27000 series, about fifty of which have been published so far:

1. ISO/IEC 27000:2018 - an overview and introduction to the ISO27k standards plus a glossary for the specialist vocabulary. **FREE!**
2. ISO/IEC 27001:2013 is the **I**nformation **S**ecurity **M**anagement **S**ystem requirements standard, formally specifying a certifiable ISMS. A new version is expected early in 2022.
3. ISO/IEC 27002:2013 is the code of practice for information security describing good practice information security controls. A new version is expected early in 2022.
4. ISO/IEC 27003:2017 provides pragmatic guidance on how to implement ISO/IEC 27001.
5. ISO/IEC 27004:2016 covers information security management measurement.
6. ISO/IEC 27005:2018 covers information [security] risk management.
7. ISO/IEC 27006:2015 is a guide to the process used by accredited ISMS certification bodies to verify and certify ISMS against ISO/IEC 27001. The current standard is being revised and will become part 1, with a new part 2 covering certification of PIMS.
8. ISO/IEC TS 27006:2021 is an accreditation standard for organizations certifying compliance of PIMS against ISO/IEC 27701.
9. ISO/IEC 27007:2020 is a guide to auditing the *management system* elements of an ISMS.
10. ISO/IEC TS 27008:2019 concerns the assessment of 'technical' security controls.
11. ISO/IEC 27009:2020 advises those producing sector- or industry-specific ISO27k standards, in effect an SC 27 internal guideline.

About the ISO27k standards

Search
Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | About us

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27009
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016

The "ISO27k" suite comprises more than seventy standards in the ISO/IEC 27000 series, about fifty of which have been published so far:

1. ISO/IEC 27000:2018 - an overview and introduction to the ISO27k standards plus a glossary for the specialist vocabulary. **FREE!**
2. ISO/IEC 27001:2013 is the **I**nformation **S**ecurity **M**anagement **S**ystem requirements standard, formally specifying a certifiable ISMS. A new version is expected early in 2022.
3. ISO/IEC 27002:2013 is the code of practice for information security describing good practice information security controls. A new version is expected early in 2022.
4. ISO/IEC 27003:2017 provides pragmatic guidance on how to implement ISO/IEC 27001.
5. ISO/IEC 27004:2016 covers information security management measurement.
6. ISO/IEC 27005:2018 covers information [security] risk management.
7. ISO/IEC 27006:2015 explains the requirements for accredited certification bodies to verify and certify ISMS against ISO/IEC 27001. The current standard is being revised and will become part 1, with a new part 2 covering certification of PIMS.
8. ISO/IEC TS 27006:2021 is an accreditation standard for organizations certifying compliance of PIMS against ISO/IEC 27701.
9. ISO/IEC 27007:2020 is a guide to auditing the *management system* elements of an ISMS.
10. ISO/IEC TS 27008:2019 concerns the assessment of 'technical' security controls.
11. ISO/IEC 27009:2020 advises those producing sector- or industry-specific ISO27k standards, in effect an SC 27 internal guideline.

Très complexe…

… donc, chronophage et coûteux

Label de qualité

CYBER SAFE

Diagnostic de cybersécurité

Cyber-safe.ch teste vos systèmes informatiques, vos collaborateurs et votre gouvernance afin d'identifier les FAILLES et VULNÉRABILITÉS pour dresser un état des lieux de votre cybersécurité.

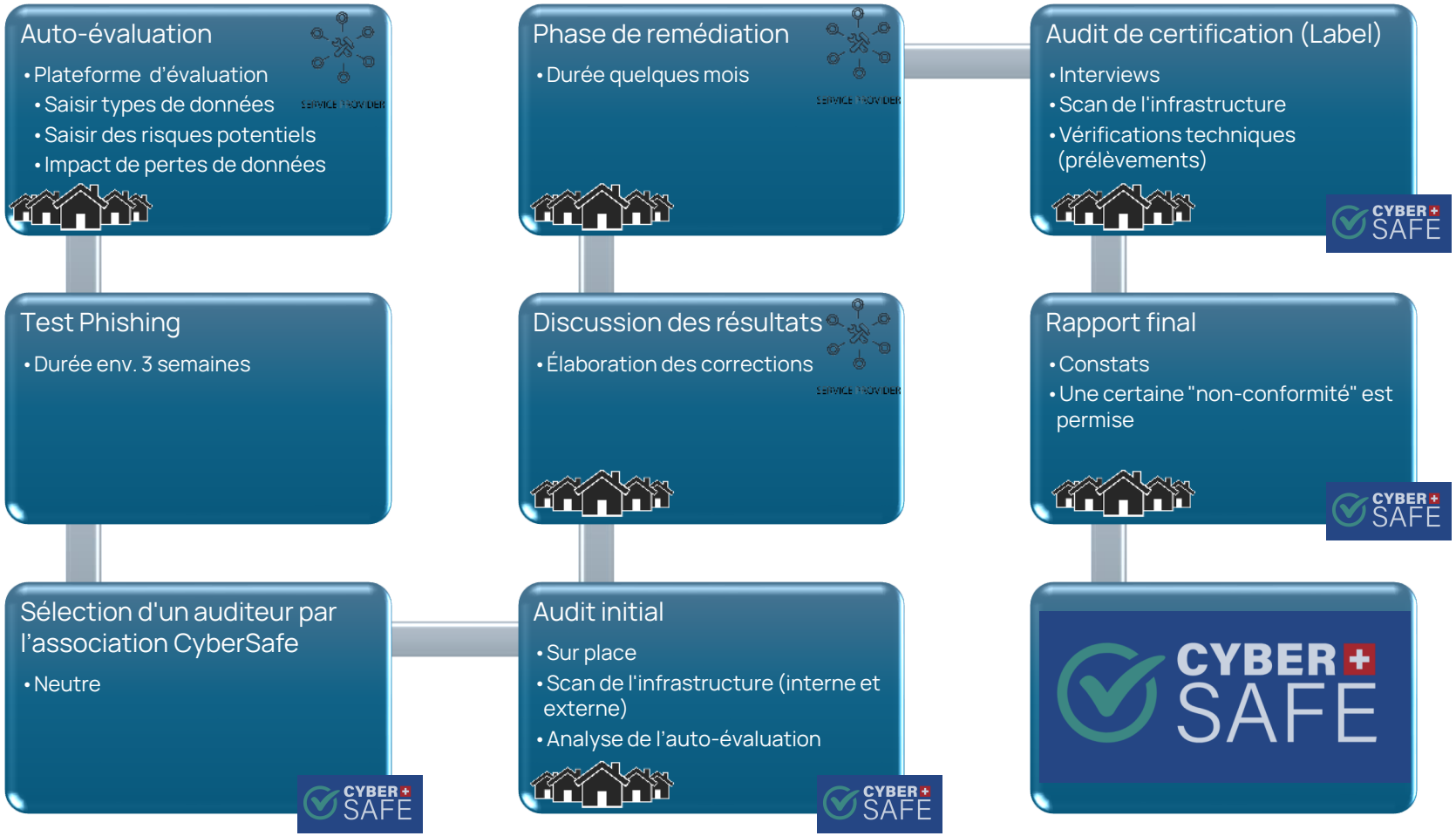
Aide à la décision

Une FEUILLE DE ROUTE pour la conduite opérationnelle (gestion des priorités selon les risques, les impacts financiers et le secteur d'activité). Sur la base de l'état des lieux, une LISTE D'ACTIONS prioritaires pour améliorer votre cybersécurité.

Cyber Audit

Cyber-safe.ch audite les candidats et vérifie que les mesures CORRECTIVES ont été appliquées. Nous contrôlons la CONFORMITE de votre cybersécurité aux exigences du Label.

CyberSafe – comment ça marche?



https://www.cyber-safe.ch

Résumé

- Déterminer la maturité actuelle en termes de cybersécurité
- Mettre en place des améliorations
  - Court terme
  - Long terme (processus, comportement)
- Sensibilisation des utilisateurs pour la cybersécurité (éducation)
- Control de la conformité aux exigences du label CyberSafe

Exemples de communes: *procédure et formation*

Bruno Marmier, Syndic, Villars-sur-Glâne

Sergio Serras, Responsable informatique, Villars-sur-Glâne

Plan de la présentation

- Etat des lieux : Infrastructure et structure informatique
- Mesures de formation des utilisateurs (personnel et élus)
- Procédure de récupération
- Label CyberSafe
- Gestion des risques

Etat des lieux : Infrastructure et structure informatique

- *Différence selon les tailles de communes*
- *Questions liées à la sécurité sont identiques*

Mesures de formation des utilisateurs (personnel et élus)

- *Rappel des dispositions légales et contractuelles*
- *Campagnes de sensibilisation sur les bonnes pratiques (mots de passe, repérer un spam, …)*
- *Exercices pratiques - Quiz*

Procédure de récupération

Bien que l'on souhaite éviter tout piratage, il convient de se préparer au cas où la commune est piratée :

- *Prévoir une procédure (cellule de crise, qui prévenir ? …)*
- *Lister les tâches affectées par un piratage et proposer des solutions*
- *Quid du personnel en cas de piratage ?*

Label Cybersafe

- *Plus-value du label Cybersafe?*

Gestion des risques

- *le responsable ou mandataire doit prendre toutes les mesures nécessaires en matière de sécurité informatique (points de repère, gestion des risques, système de contrôle interne)*

- *Mais 95% des erreurs sont humaines selon les statistiques.*

Questions – remarques?

Comment réagir en cas de suspicion d'attaque ou de menace ?

Sébastien Ruffieux, Chef de brigade, Police cantonale Fribourg

Matthieu Landert, Commissaire, Police cantonale Fribourg

Plan de la présentation

- Cybercriminalité dans le canton de Fribourg
- Comment réagir en cas de suspicion d'attaque ou de menace ?
- Rôle de la Police
- Questions?

Cybercriminalité dans le canton de Fribourg

- Augmentation des cas cyber (env. 1700 cas pour 14mio de préjudice)
- Chaque cas est différent, les scénarios évoluent, mais ils peuvent être regroupés en phénomènes
- Coordination nationale et internationale
- De nombreux liens internet, marche à suivre existent

Comment réagir en cas de suspicion d'attaque ou de menace ?

- Isoler l'appareil, déconnecter du réseau (WLAN, WIFI)
- Contacter
  - Responsable informatique interne, hiérarchie
  - Police (dénonciation pénale, récolte de traces, conseils, négociation)

- Annoncer
  - NCSC (www.ncsc.ch)
  - Association des communes (peuvent aussi subir la même attaque)
  - Déclarations obligatoires – Loi sur la sécurité de l'information (LSI art. 74b let.b)

Comment réagir en cas de suspicion d'attaque ou de menace ?

Organisation propre à la commune

- Qui est responsable / personne de contact ? Cellule de crise ?
- Faire intervenir le prestataire du service informatique !
- Informer la hiérarchie, les collaborateurs, les partenaires, …
- Coopération avec la Police
- Préparer une communication média

Le rôle de la police

- Analyse du malware et des données saisies, définir le mode opératoire, tenter d'identifier les auteurs criminels
- Conseils techniques par les spécialistes IT (pas de réparation de notre part!)
- «Coaching» pour prise de contact – échange avec les criminels (groupe négociateurs)

Le rôle de la police

- Coopération avec les autres polices cantonales, Fedpol, Europol, Interpol (souvent il y a des séries de cas)
- Dénoncer auprès du Ministère public

Questions ?

Police cantonale POL

Police de sûreté - *Kriminalpolizei*
Commissariat cybercriminalité
Place Notre-Dame 2, 1701 Fribourg
T +41 26 304 17 19, www.policefr.ch I cybercrime@fr.ch

Cyberboîte

Guide à l'intention des communes