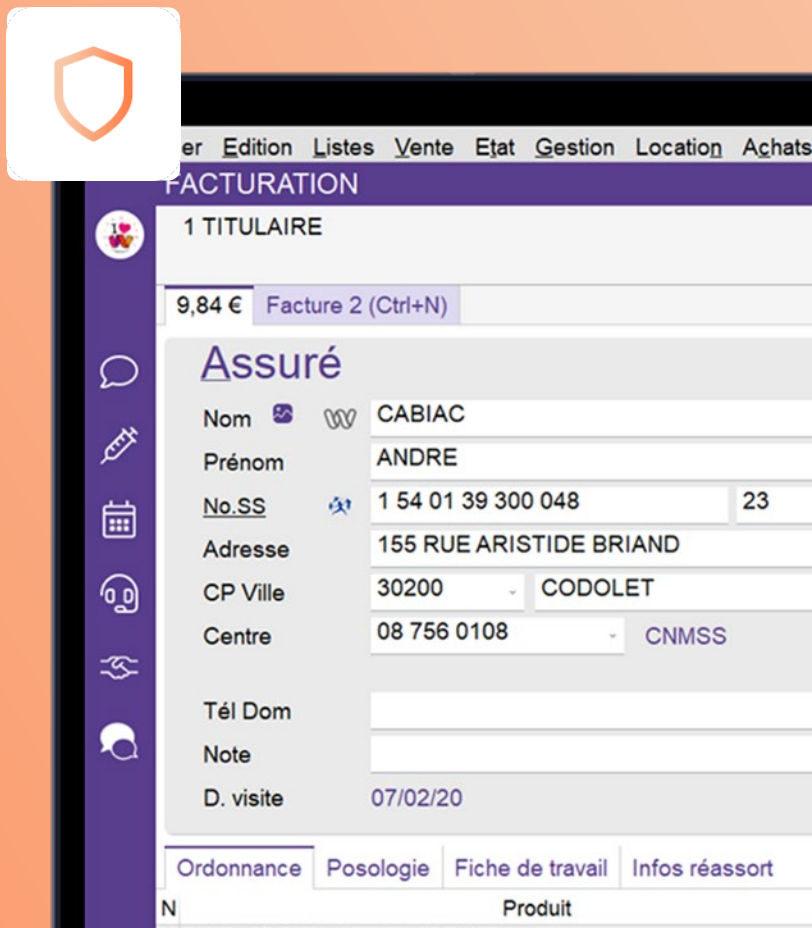
Cybersécurité

8 bonnes pratiques contre la cybermalveillance en officine



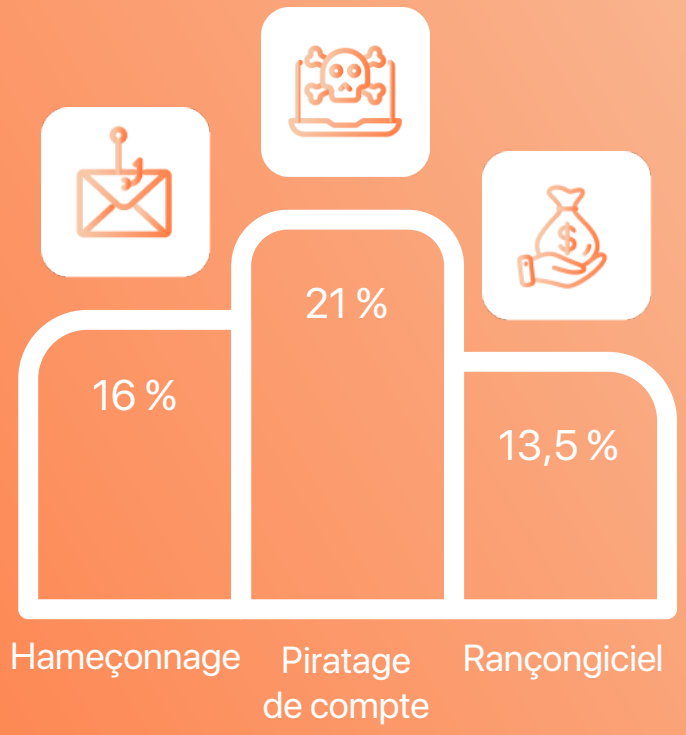
winpharma

Êtes vous prêts à faire face aux cyberattaques ?

Les cyberattaques touchent chaque année de nombreuses entreprises, mais une bonne prévention permet de réduire significativement les risques.
En 2024, ***67 % des entreprises ont été victimes d'attaques***, un chiffre en hausse et les officines ne sont pas épargnées (vol de données, piratage de messagerie, ...).

Anticiper, c'est sécuriser : en adoptant des gestes simples, vous protégez vos données, la continuité de votre activité et la confiance de vos patients.

Top 3 des cybermalveillances en 2025



Source : cybermalveillance.gouv.fr

Quels risques pour votre officine ?

Les menaces sur vos systèmes informatiques peuvent être multiples.

Les erreurs humaines involontaires

Certaines menaces proviennent d'actions quotidiennes non intentionnelles, comme :

- Un café renversé sur le clavier
- L'ordinateur laissé déverrouillé pendant une absence
- Un envoi de message au mauvais destinataire
- L'absence de sauvegardes régulières des données

Les attaques malveillantes intentionnelles

Les cybercriminels peuvent aussi causer des dommages délibérés, tels que :

- L'endommagement du matériel
- Le vol d'informations ou l'espionnage industriel
- La diffusion de virus ou de programmes malveillants
- L'usurpation d'identité et les spams

Gérez vos mots de passe avec soin.

10

Créer un mot de passe long, complexe et difficile à deviner :

- Minimum 8 caractères
- Inclure des lettres minuscules et des majuscules
- Ajouter des chiffres
- Utiliser des caractères spéciaux



Ne communiquez jamais votre mot de passe à un tiers : aucune organisation ou personne de confiance ne vous demandera de lui communiquer votre mot de passe.

Utilisez un gestionnaire de mots de passe

Il est difficile de retenir tous vos codes d'accès ! Heureusement, des outils appelés « coffres forts de mots de passe » existent. Ils enregistrent vos mots de passe et génèrent des mots de passe aléatoires pour vous.

Sauvegardez vos données.

02

Sauvegarde de données

Il est crucial d'effectuer une sauvegarde quotidienne de vos données, idéalement en fin de journée avant de quitter la pharmacie. Pour plus de sécurité, utilisez deux clés USB en les alternant tous les deux jours.

Sauvegarde à distance

Incendie, cyberattaque, vol, panne ou perte : vos données sont protégées sur des serveurs sécurisés et certifiés HDS en Europe, garantissant une récupération à tout moment. La sauvegarde en ligne est aujourd'hui la seule véritable protection contre des menaces comme les ransomwares (type Cryptolocker)

Module payant



Ne jamais laisser la clé USB branchée sur l'ordinateur !

- En cas de sinistre, elle peut être détruite avec l'ordinateur. Gardez-la avec vous.
- Si l'ordinateur est infecté, la clé le sera aussi. Débranchez-la après chaque sauvegarde.

Effectuez des mises à jour régulières

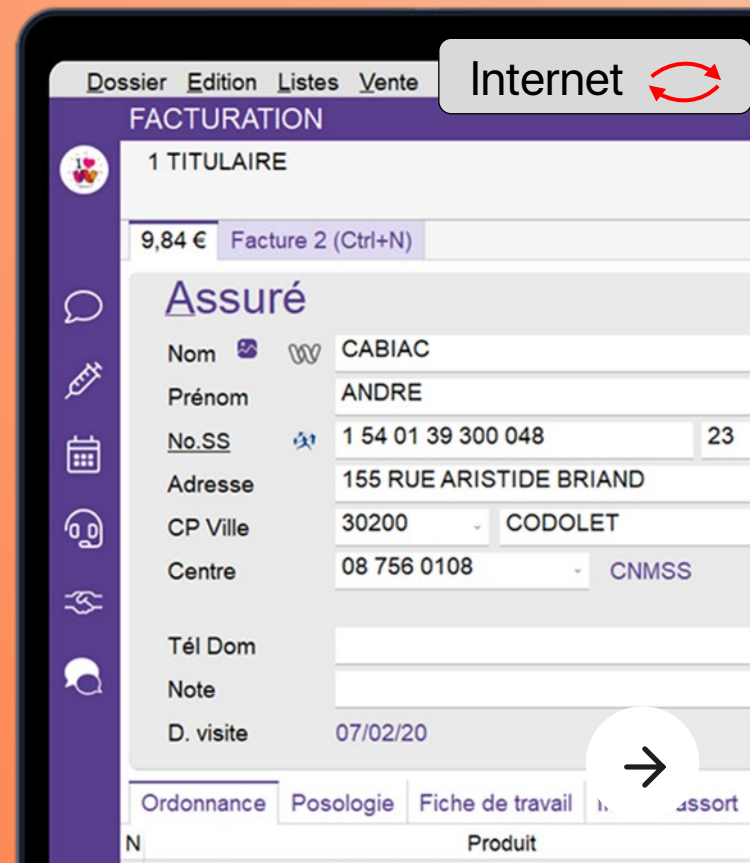
03

Gardez vos systèmes performants et sécurisés en les mettant à jour régulièrement.

Assurez-vous que vos équipements et logiciels sont toujours à jour pour garantir leur sécurité et performance. Téléchargez uniquement les mises à jour depuis des sources officielles et activez les mises à jour automatiques pour plus de simplicité.

Mises à jour Windows à effectuer

Sur Winpharma une mise à jour est indiquée par deux flèches rouges.



Protégez-vous des virus et logiciels malveillants

04

De nos jours, installer une solution de cybersécurité professionnelle est un minimum indispensable pour se protéger efficacement contre les cyberattaques telles que :

Cheval de Troie

Vol, modification ou suppression de vos données, prise de contrôle à distance de votre ordinateur.

Virus

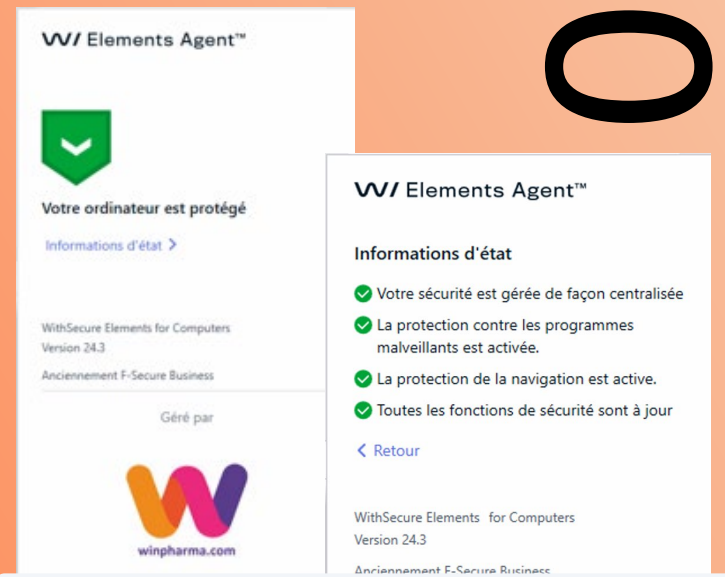
Programme qui se répand et infecte d'autres logiciels.

Rançongiciel

Demande de rançon après avoir téléchargé un fichier ou cliqué sur un email malveillant.

Pour que ces outils soient pleinement efficaces, il est important d'adopter de bonnes pratiques. Ne jamais utiliser un service ou un périphérique inconnu, comme une clé USB qui vous semble suspecte.

*EDR : Endpoint Detection & Response



Winpharma passe à la vitesse supérieure avec sa solution EDR*.

Les menaces, même inconnues ? **Repérées et bloquées automatiquement.** L'EDR veille sur vos postes 24h/24, sans ralentir vos équipements. De quoi travailler l'esprit tranquille !

Module payant

Séparez vos usages pro et perso !

05



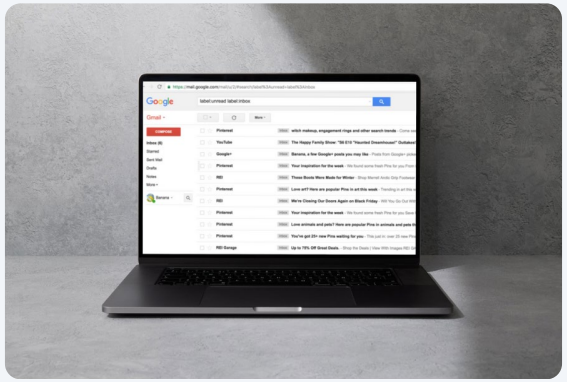
Séparer usage pro et perso

Utilisez vos équipements personnels (email, téléphone, clé USB) uniquement pour des fins personnelles et vos outils professionnels exclusivement pour le travail.



Pas de connexions non sécurisées

Ne pas brancher des clés USB ou disques durs externes dont vous ne connaissez pas la provenance. Ces supports peuvent contenir des virus ou logiciels espions.



Protéger votre email professionnel

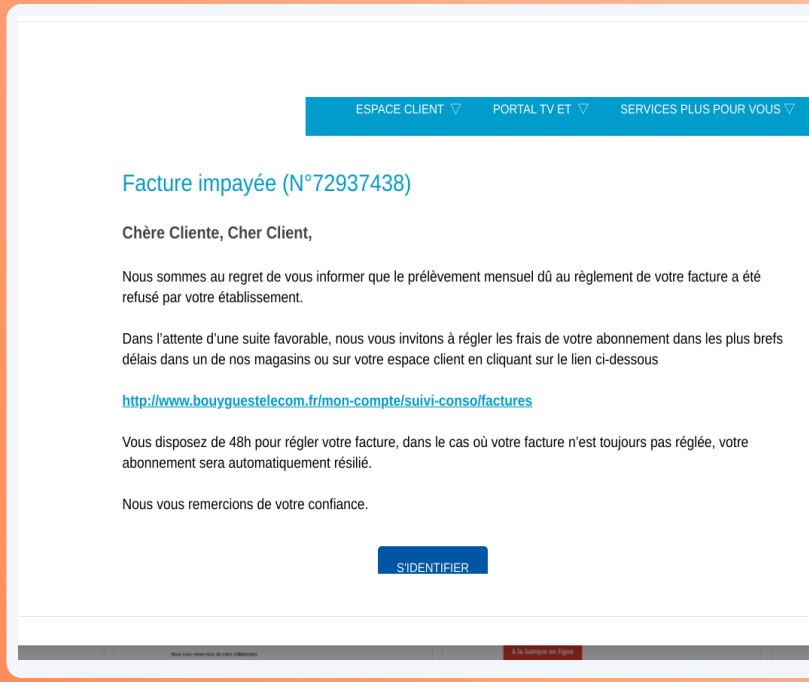
Utilisez votre email professionnel uniquement pour des fins professionnelles et ne vous inscrivez pas sur des sites personnels avec celui-ci.

Votre email, cible du phishing : Comment vous protéger ?

06

Qu'est-ce que le phishing ?

Le phishing consiste à usurper l'identité d'une organisation ou d'un proche pour voler des informations personnelles.



Règles simples à suivre :

- Vérifiez l'orthographe du contenu
- Ne cliquez pas sur des liens ou pièces jointes douteux.
- Vérifiez les liens : Passez la souris dessus pour vérifier l'adresse réelle
- Ne répondez pas à des mails suspects, contactez l'expéditeur par un autre moyen.
- Activez la double authentification si possible pour renforcer la sécurité de votre messagerie.

Protégez-vous contre les sites malveillants

07

Évitez les sites douteux, découvrez comment repérer un site web malveillant :

01 Toujours vérifier la source des liens avant de les ouvrir. Pour un e-mail, contrôlez l'expéditeur, le contenu et la signature.

02 Les hackers usurpent les URLs pour tromper. ***Un doute ? Abstenez-vous de cliquer !***

03 Un site sécurisé doit afficher un cadenas. Cliquez dessus pour ***vérifier l'authenticité du certificat SSL/TLS.***

04 Vérifiez l'ancienneté du domaine. Un site récent peut être suspect.

05 Examinez le contenu : fautes de grammaire, publicités intrusives, design suspect...

06 Recherchez des avis sur l'entreprise et le site web pour vérifier leur crédibilité et évaluer leur fiabilité.

++ Utilisez un outil comme Site Browsing Safe Status de Google pour vérifier si le site est légitime.

Ne téléchargez jamais de fichiers ***.exe*** provenant de sources inconnues. Ils peuvent contenir des virus ou des logiciels malveillants.

Limitez les accès

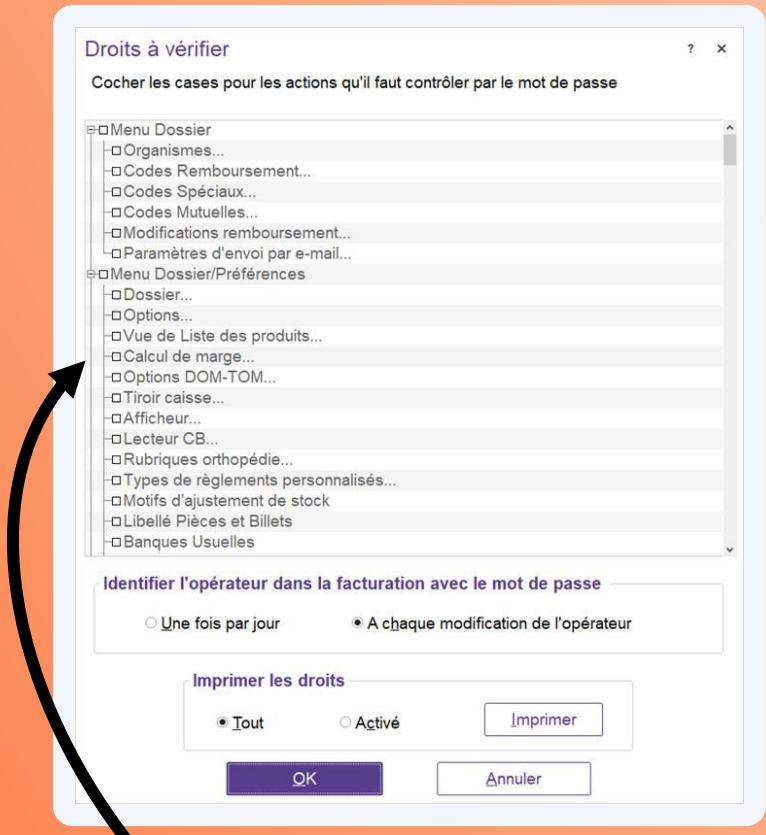
08

Pour plus de sécurité, il est recommandé ***d'ajuster les accès Winpharma selon les rôles de chacun.***

Winpharma vous permet de personnaliser facilement les droits d'accès, en activant ou désactivant certaines fonctionnalités selon le profil de l'opérateur.

Gestion des Opérateurs

Code	Nom	Nom complet	Prénom complet	No RPPS	Mot de passe	Par défaut	Par défaut pour ce poste	Journalisation	Vaccination
1	1 TITULAIRE	DAVID	GOODENOUGH		*******	☐	☐	☑	☐
2	2 OP2				*******	☐	☐	☑	☐
3	3 OP3				*******	☐	☐	☑	☐
5	5 OP5				*******	☐	☐	☑	☐
6	6 OP6				*******	☐	☐	☑	☐



Ajustez finement les droits de votre équipe

Bonnes pratiques

Prévenez les attaques avant qu'elles n'arrivent.

La cybersécurité est l’affaire de tous, protégez vos données aujourd'hui.

Tel. 0820 220 333 (0,09€ TTC/min)
contact@winpharma.com
www.winpharma.com

winpharma

Pour aller plus loin,
visionnez notre webinaire
winElearning dédié