Lettre mensuelle

Expert-comptable by Cabinet Baubet

avec expertise & conseil

12/2023

DANS CE NUMERO

Les 10 bonnes pratiques pour éviter les cyberattaques

CYBER-ATTAQUES

Nous vous présentons les 10 principaux cyber-risques et les réflexes à adopter pour se prémunir des cyberattaques :

① Hameçonnage

② Fraude au changement de RIB

③ Fraude au Président

④ Malware sur l'ordinateur d'un collaborateur de l'entreprise

⑤ Malware sur l'ordinateur d'un client

⑥ Fausse application

⑦ Mauvais choix et protection des mots de passe

⑧ Divulgation d'informations sensibles

⑨ Utilisation dangereuse d'internet

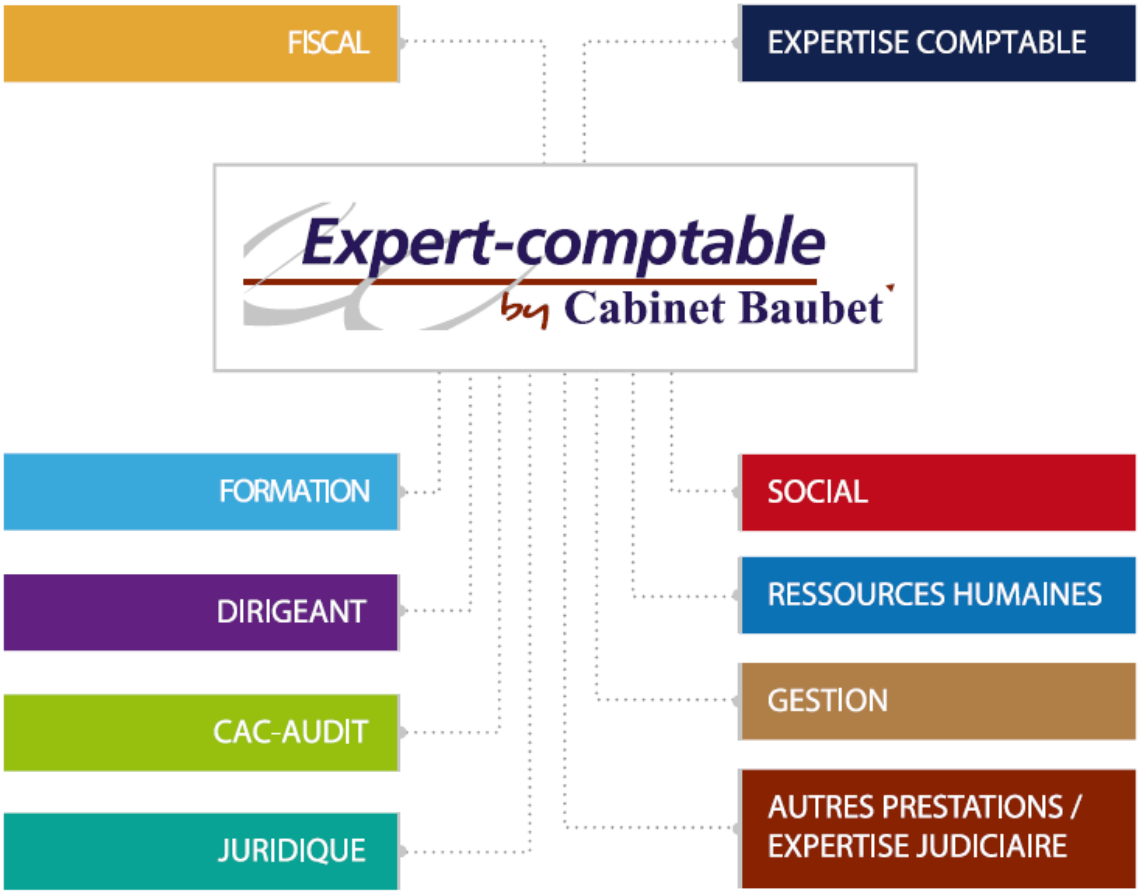
⑩ Utilisation de supports de stockages électroniques personnels ou étrangers

	Les conséquences	Les bon réflexes
① Hameçonnage		
Principe L'attaquant dispose d'informations lui permettant de contacter votre collaborateur pour lui extorquer des informations confidentielles en le dirigeant vers un autre site. Il peut envoyer un faux mail imitant celui d'une institution ou d'une entreprise, et semblant provenir d'une source fiable. **Variantes** L'hameçonnage concerne toutes les actions dont le but est d'obtenir des informations en vue d'une attaque ultérieure.	→ Pertes financières pour l'entreprise ; → Intrusion par rebond sur l'ensemble du système d'information (SI) et contamination de vos clients ; → Altération de l'image de marque ; → Conséquences judiciaires ; → Conséquences personnelles.	☑ **Si une procédure vous est inconnue ou vous paraît suspecte, vérifiez sa véracité auprès des services habilités ;** ☑ **Ne communiquez jamais d'informations sensibles par messagerie ou téléphone ;** ☑ **Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien, vérifiez l'adresse du site ; en cas de doute, contactez l'organisme concerné ;** ☑ **Respectez la charte d'utilisation SI ;** ☑ **Prévenez l'entreprise, son responsable hiérarchique au moindre soupçon.**
② Fraude au changement de RIB		
Principe L'attaquant se fait passer pour un de vos fournisseurs. Il vous signifie son changement de RIB afin d'intercepter les règlements effectués auprès du vrai fournisseur. **Variantes** L'attaquant se fait passer pour la banque ou le trésor public pour récupérer vos coordonnées bancaires.	→ Pertes financières pour l'entreprise ; → Altération possible de l'image de marque ; → Conséquences judiciaires ; → Conséquences personnelles.	☑ **Renforcez les procédures internes et particulièrement celles de confirmation des banques, modification des RIB fournisseurs et la bonne séparation des fonctions ;** ☑ **Vérifiez l'identité du fournisseur et faites un contre-appel vers un numéro déjà référencé ;** ☑ **Ne vous contentez pas des informations affichées sur les emails, ne cliquez pas sur les liens, gardez un esprit critique ;** ☑ **Méfiez-vous des emails urgents ;** ☑ **Sensibilisez vos équipes sur ce risque majeur.**

	Les conséquences	Les bon réflexes
③ Fraude au Président		
Principe Par téléphone, l'attaquant vous demande d'effectuer une opération urgente (généralement un virement). **Variantes** L'attaque peut concerner toutes les actions dont le but est d'obtenir de vous des informations qui permettront une attaque ultérieure.	→ Pertes financières pour l'entreprise ; → Altération de l'image de marque ; → Conséquences judiciaires ; → Conséquences personnelles.	☑ **Ne faites rien dans l'urgence si cela n'est pas conforme à une procédure établie ;** ☑ **Prévenez l'entreprise, votre responsable hiérarchique, de l'existence de l'attaque ;** ☑ **Redoublez de vigilance pendant les congés scolaires et jours fériés.**
④ Malware sur l'ordinateur d'un collaborateur de l'entreprise		
Principe Vous recevez un mail vous encourageant à télécharger une mise à jour de sécurité (Windows, Antivirus...) qui installera un logiciel espion sur votre ordinateur. **Variantes** Ce mail peut aussi vous encourager à consulter une page internet dans laquelle vous devez accepter l'exécution d'un script. Il peut également contenir une pièce jointe.	→ Prise de contrôle silencieuse de votre poste informatique ; → Intrusion par rebond sur l'ensemble du SI ; → Attaques induites par l'intrusion sur votre poste informatique.	☑ **Ne téléchargez pas de programmes si vous n'êtes pas certain de son origine ;** ☑ **N'acceptez pas d'invitation à consulter un site internet si vous n'êtes pas certain de son origine ;** ☑ **Interdisez les installations de logiciels.**
⑤ Malware sur l'ordinateur d'un client		
Principe Votre client a téléchargé un malware qui trompe son navigateur internet, en redirigeant sa connexion au site de l'entreprise vers un site dont le pirate a la maîtrise. **Variantes** Pas de variante.	→ Récupération des identifiants de connexion du client ; → Réalisation d'opérations préjudiciables au client et à l'entreprise ; → Altération de l'image de sécurité de l'entreprise.	☑ **Si votre client vous informe que son navigateur a été piraté, demandez immédiatement la modification de ses codes d'accès ;** ☑ **Prévenez l'entreprise et l'ensemble des collaborateurs de l'attaque.**

	Les conséquences	Les bon réflexes
⑥ Fausse application		
Principe Vous téléchargez sur le téléphone professionnel une appli non officielle, réplique de l'originale et dont l'objectif est de dérober des identifiants de connexion. **Variantes** Le téléchargement peut faire suite à l'envoi d'un mail d'hameçonnage.	→ Récupération des identifiants de connexion ; → Récupération d'informations confidentielles de l'entreprise ; → Réalisation d'opérations préjudiciables à l'entreprise ; → Altération possible de l'image de marque.	☑ **Ne téléchargez jamais d'application non officielle ;** ☑ **Soyez vigilant sur les accès demandés par les applications (liste de contacts, géolocalisation, photos...) ;** ☑ **Prévenez l'entreprise et l'ensemble des collaborateurs si vous suspectez quelque chose ou en cas d'attaque.**
⑦ Mauvais choix et protection des mots de passe		
Principe Vous choisissez des mots de passe personnels simples et vous les notez dans un fichier, un carnet ou un post-it. **Variantes** Vous communiquez le mot de passe à un collègue pour lui faciliter l'accès à un dossier partagé, ou à un proche collaborateur « au cas où ».	→ Découverte facile par un attaquant de vos accès confidentiels ; → Attaques sur votre espace de travail et par rebond sur le SI ; → Engagement de votre responsabilité personnelle.	☑ **Renforcez votre politique de gestion des mots de passe (12 caractères, avec majuscule / minuscule / chiffres / caractères spéciaux, n'ayant aucun lien avec vous, à renouveler régulièrement, etc.) .** ☑ **Ne stockez jamais vos mots de passe de manière accessible ;** ☑ **Ne les communiquez jamais ;** ☑ **N'utilisez pas d'autres comptes que le vôtre ;** ☑ **Vous devez participer à la protection des informations de l'entreprise et êtes responsable des droits que vous pourriez donner à d'autres utilisateurs.**

	Les conséquences	Les bon réflexes
⑧ Divulgation d'informations sensibles		
Principe Au travers d'anecdotes, vous dévoilez des informations sensibles pouvant être divulguées par vos interlocuteurs. **Variantes** Vous travaillez sur un appareil nomade, des documents papier, au téléphone, entouré de personnes étrangères. Votre activité est « captable ».	→ Divulgation d'informations sensibles, voire confidentielles, à de potentiels attaquants ; → Risque de préjudice pour l'entreprise ; → Engagement de votre responsabilité personnelle.	☑ **Ne parlez jamais des données personnelles de vos clients ou de procédures internes avec des tiers non autorisés ;** ☑ **Ne diffusez aucune anecdote susceptible d'altérer l'image de marque de l'entreprise, ni aucune pratique sensible propre à l'entreprise ;** ☑ **Ne laissez jamais un tiers non autorisé visualiser vos documents de travail.**
⑨ Utilisation dangereuse d'internet		
Principe Vous utilisez votre poste de travail pour vous connecter à des réseaux sociaux, des messageries instantanées, ou des sites prohibés. **Variantes** Pas de variante.	→ Risque de contamination de votre poste de travail ; → Risque de préjudice pour l'entreprise ; → Engagement de votre responsabilité personnelle.	☑ **Utilisez internet pour vos seuls besoins professionnels ;** ☑ **N'interconnectez jamais un appareil personnel avec votre poste de travail.**
⑩ Utilisation de supports de stockages électroniques personnels ou étrangers		
Principe Vous branchez une clé USB que vous venez de trouver ; elle peut contenir des programmes auto-exécutables capables de nuire à votre poste et à ceux connectés au réseau. **Variantes** Valable pour l'ensemble des supports électroniques et appareils de stockage personnels.	→ Risque de contamination de votre poste de travail et du SI ; → Risque de préjudice pour l'entreprise ; → Engagement de votre responsabilité personnelle.	☑ **Ne tentez jamais de connecter votre poste de travail à un support de stockage externe, sauf si celui-ci fait partie de vos outils de travail strictement personnels et non cessibles ;** ☑ **Utilisez exclusivement des clés USB sécurisées, fournies par l'entreprise ; conservez-les dans un coffre, sous clé...**



Expert-comptable by Cabinet Baubet

Clermont-Ferrand - 91, avenue de Royat - BP 34 63401 CHAMALIERES Cedex
Paris - 53 bis, rue de Passy 75016 PARIS
Tél. : 04.73.19.01.23 - www.**cabinet-baubet**.com

avec expertise & conseil