> cnci

Forum neuchâtelois
sur la cybersécurité

LE CYBER QUIZZ

24
questions à partager avec vos équipes

Téléchargez
le CYBER QUIZZ
complet en scannant
le QR code

Intervenants & Experts

police ello UDITIS VAV ELCASecurity helvetia

Partenaire principal

Qualibroker
Swiss Risk & Care

Forum neuchâtelois
sur la cybersécurité
LE CYBER QUIZZ

>cnci

Et vous, auriez-vous les bons réflexes ?

Un courriel suspect. Un appel urgent du CEO. Un mot de passe trop évident. Un Wi-Fi public. Une demande inhabituelle. Une pièce jointe attendue… mais pas tout à fait rassurante.

Les cybermenaces ne ressemblent pas toujours à des attaques spectaculaires. Elles se glissent souvent dans des situations très ordinaires, au cœur de nos habitudes de travail. Et dans ces moments-là, ce ne sont pas uniquement les outils informatiques qui font la différence : ce sont surtout les bons réflexes.

Ce CYBER QUIZZ vous invite à tester vos connaissances à travers des situations concrètes inspirées du quotidien des entreprises. Phishing, intelligence artificielle, protection des données, mots de passe, sauvegardes, fraude, réseaux Wi-Fi ou encore gestion des incidents : sauriez-vous repérer les pièges et avoir la bonne réaction ?

L'objectif n'est pas de devenir expert en cybersécurité, mais de mieux comprendre les risques, d'ouvrir la discussion et de renforcer, ensemble, les comportements qui peuvent réellement protéger votre organisation.

À vous de jouer.

01.

Conformité nLPD / responsabilité cloud

Question :

Votre fournisseur cloud signe un contrat stipulant qu'il est « seul responsable de la sécurité des données hébergées ». Que vaut cette clause face à la LPD ?

A) Elle est pleinement valable et vous décharge de toute responsabilité

B) Elle est valable uniquement si le fournisseur est certifié ISO 27001

C) Elle ne change rien : vous restez responsable du traitement vis-à-vis du préposé à la protection des données

D) Elle est valable si le fournisseur est domicilié en Suisse

02.

IA / Deepfake

Question :

Laquelle des 4 images est générée à l'aide de l'intelligence artificielle ?

Réponse : C
Argumentation : Les progrès dans la génération d'images ou de vidéos sont impressionnants. Il est très difficile de détecter les images générées par l'IA. Dans notre cas, il ne faut pas se fier à la qualité d'image. Nous avons expressément demandé une réduction de la qualité et une augmentation de l'authenticité. Nous avons généré l'image C en donnant les 3 autres images. Nous remarquons assez facilement les similitudes entre la B et la C.

Réponse : C
Argumentation : Art. 9 nLPD : la responsabilité du traitement est inaliénable. Vous pouvez contractualiser des obligations et des pénalités envers votre fournisseur, mais vous ne pouvez pas lui transférer votre responsabilité légale vis-à-vis des personnes concernées et du Préposé fédéral à la protection des données et à la transparence (PFPDT). Cette clause rassure — elle ne protège pas.

03.

Mises à jour / patch management

Question :

Une vulnérabilité critique est publiée un mardi matin sur le registre CVE (Common Vulnerabilities and Exposures). En moyenne, combien de temps faut-il aux groupes de ransomware pour l'exploiter activement ?

A) Entre 3 et 6 mois — le temps de développer un exploit fonctionnel
B) Entre 2 et 4 semaines — le temps que la faille se répande dans la communauté
C) Entre 15 et 30 jours — le délai standard des équipes de patch management
D) Moins de 5 jours — parfois moins de 24 heures pour les failles critiques

Réponse : D
Argumentation : Mandiant Threat Intelligence 2024 : le délai médian entre publication d'un CVE critique et première exploitation active est passé de 32 jours en 2021 à moins de 5 jours en 2024. Pour les failles les plus critiques, des exploits circulent parfois en moins de 24 heures. Ce chiffre rend caduque toute politique de patch « mensuel ».

04.

Mots de passe et authentification

Question :

Sandra travaille chez un horloger à La Chaux-de-Fonds. Son mot de passe pour accéder au logiciel de gestion des commandes est « ChxFond$2300 ». Pourquoi est-ce risqué ?

A) Il contient le nom de la ville, facilement devinable par quelqu'un qui connaît l'entreprise
B) Il est trop long, les systèmes préfèrent les mots de passe courts
C) Les chiffres en fin de mot de passe sont interdits
D) Ce mot de passe est en réalité très sécurisé

Réponse : A
Argumentation : Un attaquant qui sait que Sandra travaille à La Chaux-de-Fonds tentera naturellement des variantes du nom de la ville avec le numéro postal. Les logiciels de craquage testent automatiquement des milliers de combinaisons géographiques. Un bon mot de passe serait une phrase aléatoire, longue, mémorisable et sans lien avec le lieu de travail. Nous recommandons l'utilisation d'un logiciel coffre-fort de mot de passe comme Bitwarden par exemple qui génère des mots de passe aléatoires.

05.

Assurance cyber et gestion du risque

Question :

En termes de probabilité ET d'impact combinés, comment est perçu le risque cyber par rapport aux risques traditionnels pour une PME suisse en 2026 ?

A) Derrière l'incendie et les risques financiers, mais devant le cambriolage
B) Il est considéré comme un risque important, mais avec un impact inférieur aux risques traditionnels
C) Il est considéré comme le risque n°1, devant notamment les risques liés à l'IA et à l'interruption d'activité
D) Moins fréquent que les cambriolages, mais avec un impact financier supérieur

Réponse : C
Argumentation : Le risque cyber occupe une place centrale dans la perception des risques des entreprises. Selon l'Allianz Risk Barometre 2026, le cyber est, pour la 5ème année consécutive, le risque n°1. En Suisse, il est devant l'IA et l'interruption d'activité. Pour une PME, une cyberattaque peut cumuler plusieurs impacts : interruption d'activité, pertes financières, atteinte aux données, coûts de restauration, responsabilité vis-à-vis des tiers et atteinte à la réputation. Ce n'est plus uniquement un sujet informatique, mais un véritable risque d'entreprise.

06.

BEC / Deepfake vocal

Question :

Votre CFO reçoit un appel vocal. La voix ressemble trait pour trait à celle du CEO : « Je suis en réunion confidentielle à Zurich, j'ai besoin d'un virement de CHF 120'000.- d'ici 16h sur un nouveau compte fournisseurs. Ne passez par personne d'autre. » Votre CFO hésite. Quel est l'indice le plus révélateur que c'est une fraude ?

A) Le CEO demande un virement de CHF 120'000.-
B) La demande combine urgence, confidentialité et un nouveau bénéficiaire inconnu
C) Il est bien censé être à Zurich ce jour-là, mais ne passe généralement pas d'appels
D) La qualité audio de l'appel est légèrement dégradée

Réponse : B
Argumentation : Même si la voix ressemble parfaitement à celle du CEO, une demande de virement urgente vers un nouveau compte ne devrait jamais être exécutée sans vérification. La bonne pratique consiste à appliquer la procédure interne et à confirmer la demande par un second canal indépendant (appel sur un numéro connu, Teams, courriel professionnel ou validation par une seconde personne). Dans une attaque par Deepfake, il ne faut pas chercher à savoir si la voix est authentique. Il faut vérifier si la demande respecte les procédures et les contrôles habituels.

07.

Assurance cyber et exclusions

Question :

Votre comptable, convaincu d'avoir parlé au CEO, effectue un virement de CHF 120'000 vers un nouveau bénéficiaire. L'argent disparaît. Trois semaines plus tard, votre assurance cyber refuse d'indemniser. Quelle peut être la raison du refus ?

A) La fraude au président n'est jamais couverte par une assurance cyber
B) Le virement a été effectué volontairement ; il n'est donc, par définition, jamais couvert
C) Les conditions d'assurance peuvent prévoir des exigences spécifiques, notamment en matière de procédures, de validation ou de contrôles internes, dont le non-respect peut entraîner une limitation ou un refus de couverture
D) L'employé aurait dû détecter la voix synthétique ; faute grave caractérisée

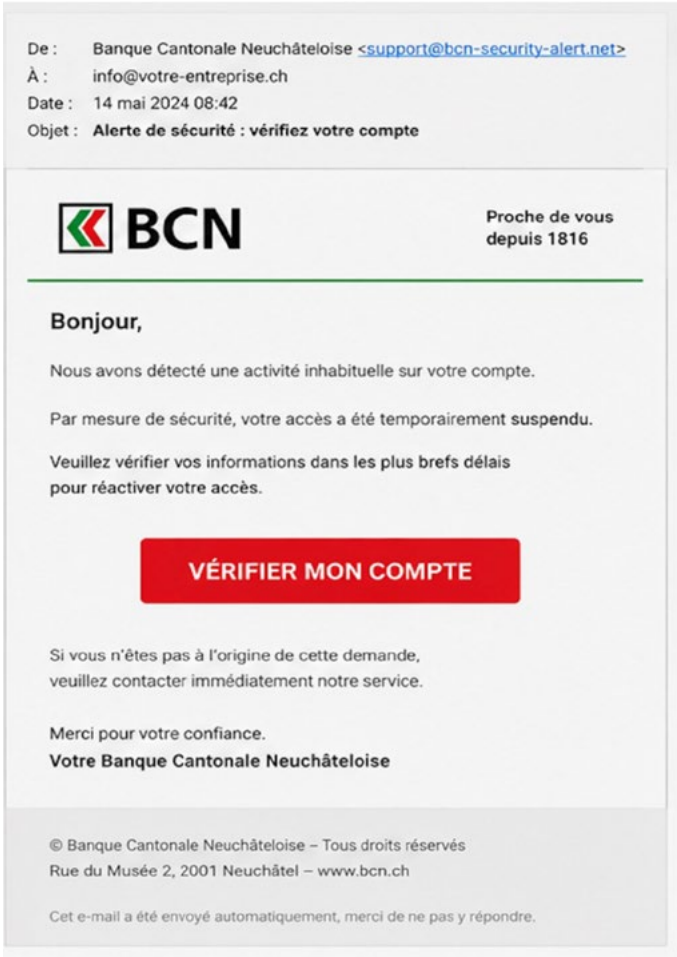
Réponse : C
Argumentation : Attention, une assurance cyber est un contrat. Qui dit contrat, dit conditions et obligations. Certaines polices peuvent prévoir des procédures de contrôle et/ou exiger des validations de paiement. Le preneur d'assurance doit être attentif à ces points. Il s'agit toujours de regarder précisément les garanties, exclusions, sous-limites et obligations prévues dans la police. Deux assurances cyber peuvent traiter une même fraude de manière différente.

08.

Phishing

Question :

Repérez les signaux d'alarme dans ce faux courriel de « BCN-services.net ».



De : Banque Cantonale Neuchâteloise <support@bcn-security-alert.net>
À : info@votre-entreprise.ch
Date : 14 mai 2024 08:42
Objet : **Alerte de sécurité : vérifiez votre compte**

BCN — Proche de vous depuis 1816

Bonjour,

Nous avons détecté une activité inhabituelle sur votre compte.

Par mesure de sécurité, votre accès a été temporairement **suspendu.**

Veuillez vérifier vos informations dans les plus brefs délais pour réactiver votre accès.

VÉRIFIER MON COMPTE

Si vous n'êtes pas à l'origine de cette demande, veuillez contacter immédiatement notre service.

Merci pour votre confiance.
Votre Banque Cantonale Neuchâteloise

© Banque Cantonale Neuchâteloise – Tous droits réservés
Rue du Musée 2, 2001 Neuchâtel – www.bcn.ch

Cet e-mail a été envoyé automatiquement, merci de ne pas y répondre.

Argumentation : Comparer le vrai domaine de la banque au domaine usurpé, rappeler qu'un logo ne prouve rien, et que la règle absolue est de vérifier l'adresse exacte de l'expéditeur et d'appeler la banque au numéro officiel plutôt que de cliquer.

09.

Bonnes pratiques organisationnelles

Question :

Un technicien quitte l'entreprise vendredi après-midi après une grave altercation avec la direction. Son accès VPN et ses identifiants courriel sont toujours actifs le lundi suivant. Quel est le risque ?

A) Aucun, un ex-employé ne ferait jamais de mal à son ancien employeur
B) Il peut accéder à distance aux fichiers techniques, données clients et systèmes internes pendant le week-end
C) Le risque est uniquement si l'employé avait des droits administrateurs
D) Les VPN expirent automatiquement après 48h

Réponse : B
Argumentation : Les accès d'un ex-employé (surtout parti dans de mauvais termes) doivent être révoqués le jour même, idéalement dans l'heure suivant le départ. Des cas documentés montrent des ex-employés ayant effacé des données, exfiltré des fichiers clients ou installé des backdoors après leur départ. Solution: une checklist d'offboarding (révocation VPN, courriel, outils métiers, récupération des équipements, changement des mots de passe partagés).

10.

Sauvegardes et continuité

Question :

Une fiduciaire n'a jamais testé la restauration de ses sauvegardes. Lors d'une panne, elle découvre que les sauvegardes sont corrompues depuis 3 mois. Quelle leçon en tirer ?

A) Les sauvegardes automatiques fonctionnent toujours, c'est la panne qui était anormale
B) Une sauvegarde non testée régulièrement n'est pas une sauvegarde fiable — les tests de restauration sont obligatoires
C) Il suffit d'augmenter la fréquence des sauvegardes pour éviter ce problème
D) Ce type de corruption est extrêmement rare et ne justifie pas des tests réguliers

Réponse : B
Argumentation : Les sauvegardes silencieusement défaillantes sont un cauchemar réel pour de nombreuses PME. Causes fréquentes : espace disque saturé, erreur de configuration, changement de logiciel non pris en compte. Règle : tester la restauration d'un fichier aléatoire chaque semaine, et un test complet au moins deux fois par an. Une sauvegarde non testée est une responsabilité de gouvernance, pas un détail technique.

11.

Gestion des incidents

Question :

Un site e-commerce a été piraté et redirige les clients vers un faux site. La première réaction du gérant est de publier un post Facebook pour prévenir ses clients. Est-ce suffisant ?

A) Oui, Facebook est le moyen le plus rapide pour toucher ses clients
B) Non, il faut aussi désactiver le site immédiatement, contacter son hébergeur, signaler à l'OFCS, et informer les clients par courriel directement si leurs données ont été exposées
C) Oui, à condition de le publier en 3 langues
D) Non, il ne faut pas communiquer publiquement pour ne pas inquiéter les clients

Réponse : B
Argumentation : La communication sur Facebook ne suffit pas : beaucoup de clients ne le verront pas, et le site compromis continue à faire des victimes pendant ce temps. Actions prioritaires : mettre le site hors ligne via l'hébergeur, changer tous les mots de passe d'administration, signaler sur ofcs.admin.ch, informer le PFPDT si des données clients ont fuité, et communiquer directement par courriel aux clients concernés.

12.

Bonnes pratiques

Question :

« La cybersécurité n'est pas un projet, c'est un processus continu. » Qu'est-ce que cela signifie concrètement pour une PME ?

A) Il faut recruter un expert cybersécurité à temps plein, sinon on ne peut rien faire
B) Sécuriser une PME, c'est adopter des bonnes pratiques durables : mises à jour régulières, formations récurrentes, revue annuelle des accès, et veille sur les nouvelles menaces
C) Une fois la première formation faite, l'entreprise est protégée pour plusieurs années
D) Seules les grandes entreprises peuvent maintenir un processus continu

Réponse : B
Argumentation : La cybersécurité est un marathon, pas un sprint : calendrier de mises à jour automatisé, formation annuelle de tous les employés, revue semestrielle des droits d'accès, test annuel des sauvegardes, veille via les alertes de l'OFCS. Ces gestes réguliers sont plus efficaces qu'un grand projet ponctuel.

13.

Navigation web et chiffrement

Question :

Que signifie HTTPS sur un site web ?

A) Site rapide
B) Site sécurisé (connexion chiffrée)
C) Site gratuit
D) Site officiel uniquement

Réponse : B
Argumentation : Sert d'introduction pour parler du chiffrement (au repos, en transit) et, si le temps le permet, du « Q-Day » — le jour où l'informatique quantique pourrait casser le chiffrement actuel.

14.

Réseaux et Wi-Fi

Question :

Ce réseau Wi-Fi public, est-il sûr ou pas ?

Réponse : Non
Argumentation : Un Wi-Fi public ne doit jamais être considéré comme sûr, même protégé par mot de passe. Il peut être mis en place par un acteur non légitime dans le but d'intercepter les communications. À utiliser uniquement via un VPN d'entreprise ou le partage de connexion du téléphone professionnel. De plus, le logo de la CNCI a été bricolé.

15.

Culture générale et gouvernance

Question :

À quoi correspond l'acronyme SOC en cybersécurité ?

A) Security Operations Center
B) Smart Online Control
C) Stop our Cyberattacks
D) Stay Out Cybercriminals

Réponse : A
Argumentation : Sert d'introduction à l'importance d'une approche SOC : protection, monitoring, alerting, rémédiation, threat intel.

16.

Bonnes pratiques organisationnelles

Question :

Qu'est-ce que le Shadow IT ?

A) Une attaque informatique
B) L'utilisation d'outils IT non approuvés
C) Un antivirus discret
D) Une organisation secrète évoluant dans le darknet

Réponse : B
Argumentation : Le Shadow IT désigne l'ensemble des outils, logiciels ou services utilisés dans une organisation sans l'approbation du service IT (cloud personnel, SaaS non validé, périphériques non autorisés). Enjeux : fuite de données, non-conformité réglementaire, manque de visibilité IT, vulnérabilités exploitables.

17.

Confidentialité des données et usage de l'IA

Question :

Dans la foulée du shadow IT, parlons du Shadow AI ;-)
Un comptable d'une fiduciaire à Neuchâtel colle les données financières d'un client dans ChatGPT pour lui faire rédiger un résumé de bilan plus rapidement. Quel est le principal risque ?

A) Aucun, ChatGPT ne fait que générer du texte, il ne conserve rien
B) Les données saisies peuvent être stockées et potentiellement réutilisées par le fournisseur de l'IA, hors de tout contrat de traitement conforme à la nLPD
C) Le risque n'existe que si le compte utilisé est gratuit
D) Le risque est équivalent à l'envoi d'un courriel professionnel classique

Réponse : B
Argumentation : Les outils d'IA grand public (ChatGPT, Copilot, Gemini en version gratuite ou personnelle) ne sont généralement pas couverts par un contrat de traitement des données (DPA) conforme à la nLPD. Les informations saisies peuvent servir à entraîner les modèles ou être stockées hors de Suisse, sans garantie de suppression. C'est le prolongement du Shadow IT, devenu « Shadow AI » : des employés voulant gagner du temps contournent la DSI avec des outils non validés et exposent involontairement des données très sensibles. Recommandation : adopter une politique d'usage claire, utiliser des outils d'entreprise avec DPA signé et former au réflexe essentiel : ne jamais saisir de données confidentielles dans un outil IA public.

18.

Bonnes pratiques organisationnelles

Question :

Quels risques de sécurité pouvez-vous repérer ?

Argumentation : Ecran non verrouillé, documents confidentiels visibles, mots de passe sur post-it, clé USB laissée sur le bureau. Même logique que le « visual hacking » : quelques secondes suffisent pour photographier un document sensible.

19.

Phishing / vishing

Question :

La Hotline UBS vous appelle, le numéro 0848 848 061 s'affiche sur votre téléphone, l'interlocuteur s'annonce comme étant la hotline UBS et vous informe d'une transaction douteuse sur votre compte. Que faites-vous ?

A) Je l'écoute, je lui donne accès à mon e-banking et valide une prise à distance de mon téléphone

B) Je lui fournis mon numéro de carte de crédit, ainsi que la date d'échéance et le numéro de vérification pour qu'il puisse être certain que l'on parle de la bonne carte

C) Je suis occupé, je lui demande de rappeler plus tard quand je suis disponible

D) Je lui demande un numéro de dossier, je vérifie le numéro de la hotline UBS et rappelle le bon numéro

Réponse : D
Argumentation : Le numéro affiché est usurpé (spoofing d'appel), une technique triviale et très répandue. Aucune banque ne demande de valider une prise de contrôle à distance ou de communiquer des données de carte par téléphone sur un appel entrant. La règle : raccrocher et rappeler indépendamment le numéro officiel figurant sur le site ou au dos de la carte.

20.

Phishing / spear phishing

Question :

Vous recevez un courriel provenant de l'adresse Webtransfer.ne.ch vous fournissant un lien pour télécharger un fichier. Le courriel stipule que l'expéditeur est externe à l'organisation ; néanmoins, vous connaissez la personne et attendez l'envoi d'un fichier volumineux d'un partenaire travaillant pour le canton. Comment agir ?

A) J'ouvre sans état d'âme, c'est forcément légitime

B) Je mets à la poubelle sans état d'âme, c'est forcément frauduleux

C) Si l'adresse du courriel est connue et légitime je peux le télécharger ; en cas de doute, je contacte mon partenaire pour vérifier

D) J'ai 37'666 courriels non lus, celui-ci attendra que j'aie ouvert les 37'665 autres

Réponse : C
Argumentation : Connaître l'expéditeur et attendre le fichier ne suffit pas à écarter tout risque, surtout quand le système signale un expéditeur externe inhabituel. Le réflexe correct est de vérifier l'adresse exacte et, en cas de doute, de contacter le partenaire par un canal indépendant (téléphone) avant de télécharger.

21.

Ransomware et malwares

Question :

Le serveur de fichiers d'une PME est touché par un ransomware un mardi matin. Quelle est la toute première action à effectuer ?

A) Payer la rançon immédiatement pour limiter l'arrêt d'activité
B) Déconnecter immédiatement tous les ordinateurs et serveurs du réseau pour stopper la propagation
C) Continuer à travailler sur les postes non touchés et appeler le prestataire IT dans l'après-midi
D) Redémarrer le serveur plusieurs fois pour tenter de débloquer les fichiers

Réponse : B
Argumentation : Chaque seconde compte : un ransomware moderne se propage sur le réseau en quelques minutes. Déconnecter physiquement les câbles réseau et désactiver le Wi-Fi sur tous les appareils, ne pas éteindre violemment les serveurs (preuves forensiques), appeler le prestataire IT, signaler à l'OFCS. Ne jamais payer — rien ne garantit la récupération des données.

22.

Réseaux et Wi-Fi

Question :

Lors d'un salon professionnel, un commercial se connecte au Wi-Fi « Officiel » de l'événement. Plus tard, son ordinateur envoie des données en arrière-plan. Quelle est l'explication la plus probable ?

A) Le Wi-Fi du salon était surchargé, ce qui cause des erreurs de transmission
B) Il s'est connecté à un faux point d'accès Wi-Fi (Evil Twin) imitant le réseau officiel, installé par un attaquant
C) Son antivirus effectue une mise à jour automatique
D) Le réseau du salon utilise une technologie qui envoie automatiquement des diagnostics

Réponse : B
Argumentation : Un « Evil Twin » est un faux point d'accès Wi-Fi portant le même nom qu'un réseau légitime, installé par un attaquant dans le même lieu. Les appareils s'y connectent automatiquement, permettant l'interception du trafic. Recommandation : désactiver la connexion Wi-Fi automatique en déplacement et utiliser un VPN.

23.

Gestion des incidents

Question :

Une PME subit une cyberattaque. Quelles autorités suisses peuvent être contactées pour signaler l'incident et obtenir des conseils ?

A) Uniquement Interpol, les autorités suisses ne traitent pas les cybercriminalités
B) L'OFCS (Office fédéral de la cybersécurité) pour le signalement et conseils, et la police cantonale pour les infractions pénales
C) Uniquement son prestataire IT, les autorités publiques n'interviennent pas dans les incidents privés
D) La FINMA, qui supervise toutes les cyberattaques en Suisse

Réponse : B
Argumentation : L'OFCS (ofcs.admin.ch) est le point de contact national pour les incidents cyber : signalement en ligne, guides pratiques gratuits, alertes sur les menaces en cours. La police cantonale traite les aspects pénaux. Le PFPDT doit être informé si des données personnelles sont exposées.

24.

Conformité nLPD

Question :

Un garage conserve les données de 3'000 clients (nom, adresse courriel, historique, immatriculation) dans un fichier Excel non chiffré sur un poste partagé. Suite à un piratage, ces données fuitent. Que prévoit la nLPD suisse ?

A) Rien, la nLPD ne s'applique qu'aux entreprises de plus de 50 employés
B) L'obligation d'informer les clients concernés et de signaler l'incident au PFPDT si le risque pour les personnes est élevé
C) Une amende automatique de CHF 250'000.- payable immédiatement
D) La nLPD ne s'applique pas aux données des clients, seulement aux employés

Réponse : B
Argumentation : La nLPD impose à toute entreprise suisse, quelle que soit sa taille, de protéger les données personnelles et de signaler les violations au PFPDT en cas de risque élevé. Des sanctions peuvent atteindre CHF 250'000.- pour les responsables personnes physiques.

>Informer >Sensibiliser >Soutenir

L'organisation du Forum neuchâtelois sur la cybersécurité permet à la CNCI d'informer les entreprises et PME de notre canton sur cette problématique, de les sensibiliser ainsi que de les soutenir par rapport à un phénomène qui peut paralyser des petites comme des grandes sociétés. La CNCI remercie les experts issus de l'entrepreneuriat et d'institutions étatiques ainsi que Qualibroker Swiss Risk & Care de leur précieuse contribution à l'organisation du troisième Forum neuchâtelois sur la cybersécurité et à la publication du présent CYBER QUIZZ.

Au cœur de l'économie

>cnci

Chambre neuchâteloise
du commerce et de l'industrie
Rue de la Serre 4
2000 Neuchâtel
Tél. 032 727 24 10
cnci@cnci.ch
www.cnci.ch