La chambre forte

Plan de match de la cybersécurité

Table des matières

Comment vous protéger, votre famille et vous, dans le monde numérique	4
Ne négligez pas la protection par mots de passe	6
Doublez vos mesures de sécurité	9
Huit étapes à suivre pour améliorer la sécurité de votre téléphone	12
Sécurité sur les réseaux Wi-Fi. Rien n’est gratuity en ce bas monde	14
Surpartage et géomarquage : Je t’ai trouvé !	17
Faites planer le mystère sur Internet	19
Paiement en ligne. Votre cheque a-t-il été envoyé à la mauvaise adresse ?	21
Protection des enfants en ligne	24
Glossaire	26

Signaler une cyberfraude à RBC

Si vous pensez avoir été victime d’une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d’experts dévoués vous indiquera les mesures appropriées à prendre.

Comment vous protéger, votre famille et vous, dans le monde numérique

Éducation. Communication. Préparation.

Vous est-il arrivé d’apprendre qu’on venait de lancer un nouveau modèle de téléphone intelligent alors que vous veniez tout juste d’en acheter un le mois précédent ?

Si c’est le cas, vous savez à quel point la technologie peut changer rapidement. L’évolution rapide de la technologie est formidable pour les consommateurs, mais aussi pour les cybercriminels, car les progrès techniques leur procurent de nouveaux moyens d’accéder à des renseignements sur nous. Heureusement, il existe des mesures simples à prendre pour se protéger de façon proactive.

S’il est vrai que RBC s’est engagée à veiller à la sécurité de vos renseignements financiers, ce guide contient des pratiques exemplaires qui vous aideront à vous protéger lorsque vous êtes en ligne. Il vous donnera les connaissances nécessaires pour améliorer vos aptitudes en matière de cybersécurité.

Ressources

RBC :
Soyez cyberfuté

Gouvernement du Canada :
Rester en sécurité en ligne
Introduction à l’environnement de cybermenaces

Autres : (en anglais seulement)
Protéger vos avoirs contre les pirates
Que faire en cas d’attaque de votre entreprise ou de vos employés

Ne négligez pas la protection par mots de passe

Il est temps de renouveler vos vieux mots de passe

Nous comprenons. Il peut être ennuyeux d'avoir à mémoriser de nouveaux mots de passe uniques pour tous vos comptes en ligne. Mais il est aussi ennuyeux de se faire pirater. Pour protéger vos comptes en lignes contre les cybercriminels, il est essentiel de choisir des mots de passe différents pour chacun d'entre eux. Un gestionnaire de mots de passe peut vous aider en enregistrant vos mots de passe dans une chambre forte et en vous en suggérant de nouveaux pour chaque site.

Étapes à suivre pour renforcer les mots de passe

1. **Utilisez un mot de passe different ou une phrase d'identification différente pour chacun de vos comptes,** particulièrement s'ils contiennent des renseignements sensibles ou financiers.

2. **Privilégiez la longueur à la complexité.**
Utilisez toujours l'intégralité du nombre de caractères permis.
Essayez d'avoir un mot de passe d'au moins 16 caractères, si possible.

3. **Évitez les mots ou termes communs comme « mot de passe » ou « utilisateur »,** ou toute information qui pourrait être facile à deviner telle que votre date de naissance ou une suite évidente comme « 1234 » ou « ABCD ».

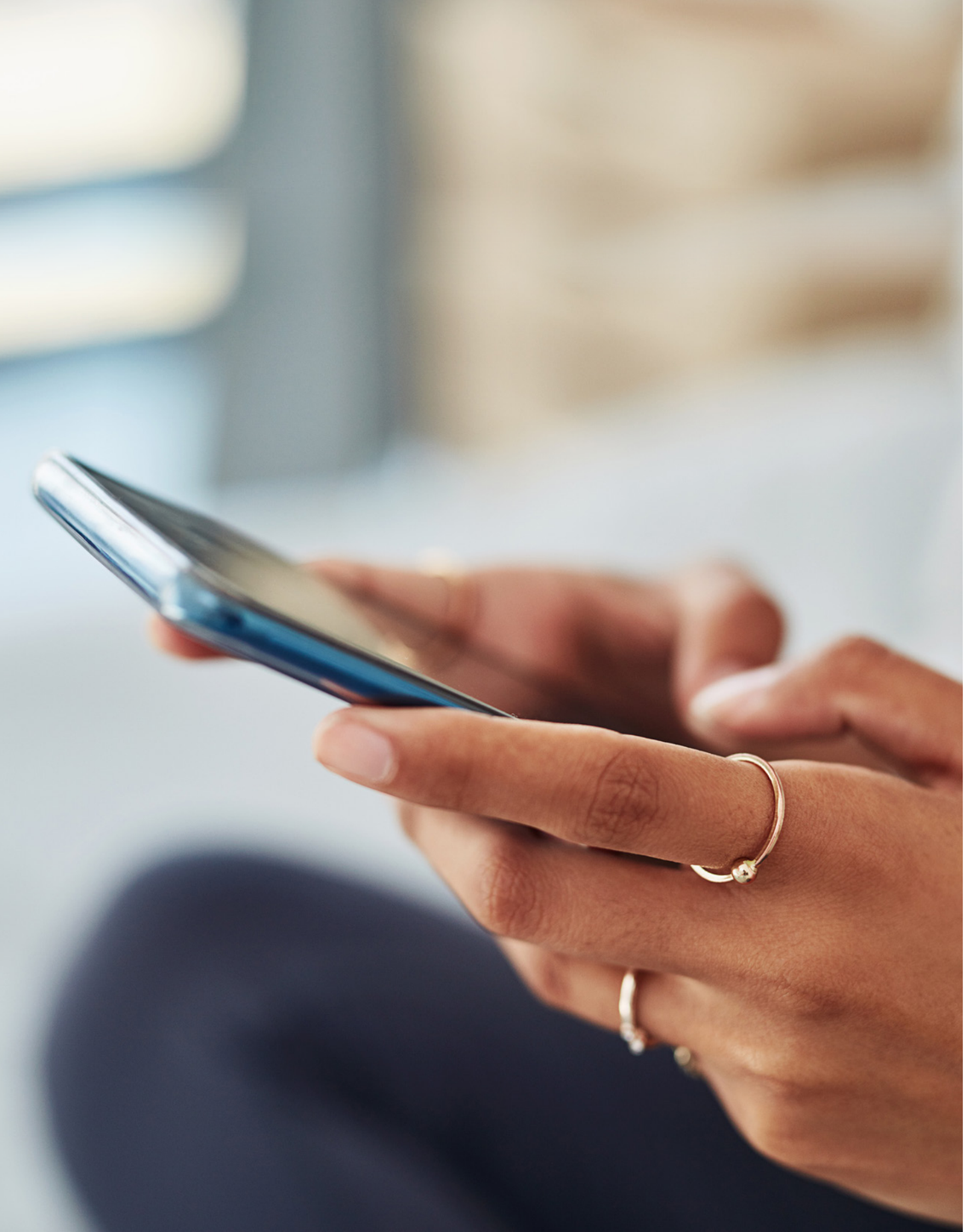
4. **Faites preuve d'originalité.**
Bien souvent, les mots de passe les plus fiables sont constitués de plusieurs mots : il s'agit alors de « phrases d'identification » composées de mots choisis au hasard. Elles peuvent être à la fois faciles à mémoriser et difficiles à deviner pour quelqu'un d'autre. « Europe Profit Maintenant » par exemple.

5. **Songez à utiliser un gestionnaire de mots de passe.**
Les gestionnaires de mots de passe génèrent des mots de passe fiables et aléatoires qu'ils mémoriseront pour vous. Vous pourrez ensuite accéder à votre base de données de mots de passe chiffrés à l'aide d'un mot de passe ou d'une phrase d'identification maître. Vous n'aurez donc à retenir qu'un seul mot de passe.

Remplacez certaines lettres par des espaces, des chiffres ou des caractères spéciaux (par exemple, @ à la place des « a » ou $ à la place des « s »), la fiabilité de votre mot de passe s'en trouvera considérablement renforcée.

Doublez vos mesures de sécurité

C’est un peu comme de poser plusieurs serrures sur votre porte.



Pour ouvrir une session dans un compte en ligne, vous devez généralement prouver votre identité en entrant un identifiant et un mot de passe. Cela offre un niveau de sécurité. Mais parfois, un niveau ne suffit pas, particulièrement lorsqu'il est question de renseignements sensibles ou financiers. C'est pourquoi de nombreux sites ont ajouté un second niveau, ou un second facteur, qui contribue à prouver que vous êtes bien la personne que vous prétendez être en vous envoyant un texto contenant un NIP ou en vous demandant une empreinte digitale. Si vous activez l'authentification multifacteur cela peut contribuer à réduire les chances que quelqu'un d'autre accède à votre compte, ce qui permet de veiller à ce que les bonnes personnes puissent ouvrir une session, mais pas les voleurs.

L’authentification multifacteur

Parfois, l’authentification multifacteur est activée automatiquement, mais il arrive aussi que vous ayez le choix de l’utiliser ou non. Si l’authentification multifacteur est offerte en option, nous vous suggérons fortement de l’utiliser. Voici comment l’activer sur certaines plateformes en vogue :

RBC

Vérification en deux étapes dans l’appli Mobile

Google

Obtenir des codes de validation avec Google Authenticator

Microsoft

Obtenir des codes de validation avec Microsoft Authenticator

Identification à deux facteurs pour les appareils Apple

Les téléphones intelligents sont intelligents, mais pas toujours sûrs

Si, comme de nombreux Canadiens, vous enregistrez la plupart des aspects de votre vie dans votre appareil mobile, comme les coordonnées des personnes que vous connaissez, vos photos, et vos comptes de médias sociaux et de courriel… Comment vous sentiriez-vous si quelqu'un piratait votre appareil et vous empêchait d'y accéder ou volait vos données personnelles ?

Huit étapes à suivre pour améliorer la sécurité de votre téléphone

Consultez ces **huit étapes simples** pour sécuriser votre appareil mobile et empêcher qu'on ne le pirate.

1. Lorsque vous n'utilisez pas le Wi-Fi, désactivez-le.
2. Installez un VPN et utilisez-le systématiquement lorsque vous vous connectez à des réseaux Wi-Fi.
3. Installez les mises à jour dès qu'elles sont disponibles.
4. Désinstallez les applications que vous n'utilisez pas et celles qui réclament trop de renseignements ou d'accès.
5. Utilisez les technologies biométriques et un mot de passe plus long pour déverrouiller votre appareil.
6. Effacez régulièrement vos paramètres de réseau pour que votre appareil « oublie » les réseaux Wi-Fi qui ne sont pas sûrs et que vous n'utilisez plus.
7. Désactivez le Bluetooth lorsque vous ne l'utilisez pas.
8. Si vous faites réparer votre appareil, réinitialisez aux paramètres par défaut avant de l'texpédier.

Conseils pour les appareils Android :

- Prévoyez des sauvegardes régulières.
- Désactivez l'accès des développeurs (il est désactivé par défaut).
- Désactivez l'accès aux boutiques d'applications de tiers (Paramètres > Recherche de « installation d'applications inconnues »).
- Activez l'outil « Localiser mon appareil » pour pouvoir localiser votre appareil et protéger vos données en cas de perte.
- Créez un mot de passe fiable pour Google.
- Activez l'authentification multifacteur pour les sites que vous visitez.

Conseils pour les appareils iOS :

- Activez la fonctionnalité « Localiser mon iPhone » pour localiser les appareils perdus ou en effacer tout le contenu.
- Désactivez la fonctionnalité « Sauvegarde iCloud », sauf si vous êtes d'accord pour que vos photos soient sauvegardées dans le nuage.
- Utilisez iTunes pour faire une sauvegarde chiffrée et enregistrer vos paramètres.
- Créez un mot de passe fiable.

Sécurité sur les réseaux Wi-Fi. Rien n’est gratuity en ce bas monde

Ce point d'accès sans fil pourrait vous causer bien des soucis

Les réseaux Wi-Fi publics sont moins sûrs que votre réseau privé parce que vous ne savez pas qui les a configurés et ni quelles sont les autres personnes qui y sont connectées. De plus, les connexions qui ne sont pas chiffrées permettent aux cybercriminels de surveiller tous les renseignements que vous échangez avec le serveur, voire d'y accéder.

Voici comment vous protéger lorsque vous utilisez un réseau Wi-Fi :

- Évitez d'accéder à des comptes renfermant des renseignements privés ou sensibles.
- Utilisez un VPN (réseau privé virtuel) sécuritaire et chiffré.
- Soyez conscient des personnes qui vous entourent ou qui pourraient regarder par-dessus votre épaule.
- Prenez toujours des précautions lorsque vous réalisez des activités en ligne, même si votre connexion Wi-Fi est sécuritaire.

Conseils pour sécuriser votre réseau Wi-Fi à la maison

1	Modifiez le nom par défaut de votre réseau Wi-Fi (SSID) et configurez un réseau invité.	• SSID sans renseignements personnels • Réseau invité distinct des appareils principaux
2	Choisissez un mot de passe réseau sans fil unique et complexe.	• Au moins 20 caractères • Des lettres, des chiffres et des symboles
3	Activez le chiffrement du réseau.	• Activez le chiffrement immédiatement après l'installation
4	Désactivez la diffusion du nom du réseau.	• Désactivez cette fonction afin de limiter l'accès à votre réseau aux seules personnes connaissant votre identifiant SSID
5	Tenez le logiciel de votre routeur à jour.	• Un micrologiciel défectueux devient une faille de sécurité • Maintenez le logiciel à jour et téléchargez les plus récents correctifs de sécurité
6	Assurez-vous d'avoir un bon pare-feu.	• Activez le pare-feu déjà intégré • Ou installez-en un bon si votre appareil n'en est pas déjà muni
7	Utilisez un VPN pour accéder à votre réseau.	• Un VPN authentifié protège les communications Internet grâce au chiffrement

Surpartage et géomarquage : Je t’ai trouvé !

Ne dévoilez pas tout en un clic

Vous aimez partager vos photos de vacances. Et vos parents et amis aiment les voir, tout comme les cambrioleurs et les escrocs. Quand vous révélez votre emplacement en voyage, vous devenez une cible pour les criminels, ce qui vous expose au risque d'usurpation d'identité, de menaces pour votre sécurité physique, de harponnage et de piratage psychologique.

Assurez-vous de vous protéger et de protéger ce qui compte pour vous.

Étapes à suivre pour vous protéger

1. Définissez vos comptes de médias sociaux comme privés.
2. Désactivez le géomarquage.
3. Renforcez vos questions de sécurité.
4. Évitez de publier des données sensibles comme des numéros de téléphone, des adresses et destinations touristiques.

Autres ressources (en anglais seulement)

Cliquer pour sécuriser vos comptes :

TikTok

Désactiver le géomarquage :

Faites planer le mystère sur Internet

Le danger de l’hameçonnage et des courriels malveillants.

Fonctionnement de l’hameçonnage

- Les courriels proviennent d’organisations ou de particuliers qui vous demandent vos renseignements personnels et financiers.
- Ils peuvent aussi bien vous faire miroiter des récompenses financières que vous menacer ou se faire passer pour une personne qui a vraiment besoin d’aide.
- Alors que vous croyez donner des renseignements à une société légitime, vous les donnez plutôt à un fraudeur.

Types d’hameçonnage

- Harponnage par texto
- Harponnage
- Harponnage vocal
- Courriel d’affaires compromis

- Données utiles
  - Logiciel malveillant
  - Logiciel espion
  - Rançongiciel

Comment vous protéger

- Vérifiez si le texte comporte des erreurs de grammaire ou d’orthographe et si le langage est inhabituel.
- N’ouvrez jamais de pièces jointes que vous ne vous attendiez pas à recevoir.
- Prenez un moment pour réfléchir avant de répondre à un courriel inattendu.
- Fiez-vous à votre instinct : si quelque chose semble douteux, ce l’est probablement.
- Si le courriel semble provenir d’une personne que vous connaissez, communiquez avec elle afin de vous en assurer.
- Ne donnez aucun renseignement personnel et n’en affichez pas non plus.

Paiement en ligne. Votre cheque a-t-il été envoyé à la mauvaise adresse ?

Évitez de vous retrouver en situation de paiement perdu dans le courrier

Pour envoyer des fonds à quelqu'un, les virements entre banques sont les plus sûrs. Mais si cette option n'est pas possible, vous devez prendre des mesures pour protéger votre argent et vos renseignements.

Mesures à prendre pour vous protéger contre le vol sur les applications de paiement pair à pair[1] :

1. Créez un mot de passe complexe lorsque vous établissez votre compte.
2. Utilisez l'autentification multifacteur, c'est-à-dire créez un NIP qui doit être saisi avant d'envoyer de l'argent.
3. Réduisez les risques en utilisant des cartes de crédit et non des cartes de débit.
4. Gérez votre application de paiement pair à pair sur un réseau sécurisé et un système d'exploitation à jour.
5. Activez les notifications de façon à être informé lorsque votre argent est reçu.
6. Fermez votre session sur l'application une fois le transfert effectué.
7. Vérifiez les détails de l'opération trois fois plutôt qu'une. Une fois que l'argent est envoyé, vous ne l'avez plus, comme lorsque vous payez en espèces.

Conseils pour éviter les escrocs de paiement pair à pair

- N'interagissez pas avec des comptes qui prétendent donner de l'argent aux utilisateurs qui partagent ou aiment des publications[2].
- Les applications de paiement pair à pair (p. ex. CashApp, Venmo ou PayPal) ne vous demanderont jamais d'argent pour « vérifier » votre compte. N'acceptez pas ces demandes[2].

Protection des enfants en ligne

Grandir en ligne comporte des avantages et des risques

Vos enfants vont passer du temps en ligne, c'est connu et même essentiel à notre époque de haute technologie. Il vous faudra donc les protéger de façon aussi vigilante et prudente dans le monde virtuel que vous le faites dans le monde reel.

Étapes à suivre pour protéger votre enfant en ligne[3]

1. Gardez les appareils à un endroit où vous pouvez les voir.
2. Configurez le contrôle parental. La fonction Filtres SafeSearch sur Google permet de bloquer des sites affichant du contenu explicite.
3. Renseignez-vous sur les amis en ligne de votre enfant.
4. Incitez votre enfant à se poser des questions : est-ce que je partagerais ces renseignements ou cette photo avec une personne que je ne connais pas ? Si la réponse est non, il ne faut pas les publier.
5. Expliquez à votre enfant comment rendre son emplacement invisible.
6. Signalez les publications inappropriées et protégez vos renseignements.

Ressources

RBC :
Comment vous protéger en ligne

Autre : (en anglais seulement)
Protection des enfants en ligne

Glossaire

Authentification multifacteur	Une méthode d'authentification électronique qui oblige l'utilisateur à respecter au moins deux facteurs d'authentification pour avoir accès à une application ou à un compte. On utilise aussi l'expression « authentification à deux facteurs » ou « A2F ».
Chiffrement	Une opération de transformation des données grâce à laquelle seuls les utilisateurs autorisés peuvent comprendre l'information. Il s'agit d'un moyen de protéger ses données sur son réseau.
Coupe-feu	Un dispositif de sécurité de réseau qui surveille le flux de données entre deux réseaux. Il autorise ou bloque le passage de données selon un ensemble défini de règles de sécurité.
Courriel d'affaires compromis	Une escroquerie par intrusion dans un courriel qui semble provenir d'une source légitime (p. ex. un haut dirigeant) et incite le destinataire à prendre des mesures immédiates comme virer des fonds ou transférer des renseignements.
Géomarquage	L'ajout d'un ensemble de données géographiques ou d'emplacements à divers médias qui permet à quiconque de déterminer où une personne se trouve.
Gestionnaire de mots de passe	Une base de données chiffrées de mots de passe qui est déverrouillée au moyen d'un mot de passe principal.
Logiciel malveillant	Un logiciel malveillant ou « maliciel » est un logiciel conçu par un cybercriminel pour subtiliser de l'information, endommager des fichiers enregistrés ou prendre le contrôle d'un ordinateur ou d'un appareil.
Paiement pair à pair	Un système de paiement lié au compte bancaire ou à la carte de crédit de l'utilisateur et qui permet à ce dernier d'envoyer et de recevoir de l'argent de son appareil mobile.
Phrase d'identification	Des groupes de mots choisis de façon aléatoire, connus de l'utilisateur et difficiles à deviner pour un pirate (p. ex. Délai Éléphant Acheter).
Réseau Wi-Fi invité	Un point d'accès sur votre réseau, distinct de celui auquel vos principaux appareils se connectent. Ainsi, des appareils plus exposés aux virus informatiques ont accès à Internet par le biais du réseau invité sans avoir à se connecter à votre réseau.

Terminal de paiement spécialisé	Des appareils sous gestion indépendante utilisés dans un but précis, par exemple à la caisse d'un magasin et aux guichets automatiques bancaires.
Rançongiciel	Un logiciel malveillant conçu pour bloquer l'accès à un ordinateur dans le but d'extorquer de l'argent à l'utilisateur pour lui en rendre l'accès.
Cheval de Troie d'accès à distance	Un programme qui permet à un intrus de prendre le contrôle d'un ordinateur afin d'exécuter des activités malveillantes.
Nom de réseau sans fil (SSID)	Le terme technique qui désigne le nom de réseau Wi-Fi.
Hameçonnage par texto	Un type d'hameçonnage qui cible les téléphones cellulaires. Cette escroquerie utilise les messages textes pour inciter une personne à cliquer sur des liens ou à télécharger des pièces jointes qui installeront des logiciels malveillants ou tenteront de voler ses renseignements personnels ou financiers.
Piratage psychologique	Une tromperie qui vise à manipuler une personne afin qu'elle divulgue des renseignements confidentiels ou personnels dans le but de commettre une fraude.
Harponnage	Un type d'hameçonnage qui cible de façon précise un individu. Les messages peuvent ressembler à ceux d'un ami ou d'un parent et contenir des renseignements précis sur lui ou l'organisation avec laquelle il traite.
Logiciel espion	Un logiciel conçu pour pénétrer dans un appareil, recueillir des données et les transmettre à un tiers. Ce logiciel, qu'il soit malveillant ou légitime, s'intéresse aux données à des fins commerciales.
Réseau privé virtuel (VPN)	Un groupe d'ordinateurs ou de réseaux qui fonctionnent ensemble sur Internet afin de protéger les communications, par exemple en les chiffrant.
Hameçonnage vocal	Cette technique d'hameçonnage utilise le téléphone pour tenter de commettre une fraude ou de dérober des renseignements sensibles à la personne qui répond.

Ressources

1. Real Simple. 2018. *This Is Exactly How to Avoid Hackers When Using Venmo and PayPal* (en anglais seulement). 7 juillet 2022. <https://www.realsimple.com/work-life/technology/safety-family/money-sharing-app-safety>

2. Tenable. 2020. *Scams Exploit COVID-19 Giveaways Via Venmo, PayPal and Cash App* (en anglais seulement). 7 juillet 2022. <https://www.tenable.com/blog/scams-exploit-covid-19-giveaways-via-venmo-paypal-and-cash-app>

3. Gouvernement du Queensland. 2017. *10 Things Every Parent can do to Keep Their Kids Safe Online* (en anglais seulement). 7 juillet 2022. <https://www.childrens.health.qld.gov.au/blog-10-things-keep-kids-safe-online/>

128677 (10/2022)