CYBERSÉCURITÉ

NOUS SOMMES TOUS CONCERNÉS

PDF

Sur ordinateur, smartphone ou internet, adopte les bons réflexes !



IFSB

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

CHAMBRE DES METIERS
Luxembourg

Cybersécurité n°3 : Virus

LES GESTES BARRIERES DU NUMERIQUE

En adoptant les bon gestes barrières il est possible de se protéger des menaces numériques et de limiter les impacts d'une attaque sur les systèmes d'informations

🔐 Choisi un très bon mot de passe

- Choisi des mots de passe composés si possible de 8 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux)
  Exemple : ght5CD%7
- Défini un mot de passe unique pour chaque service sensible (banque, messagerie…)

📸 Fais attention au partage de photos et vidéos ; elles contiennent beaucoup d'informations

- En partageant des médias sur les réseaux sociaux beaucoup de monde y aura accès.
- Des informations visibles dans la photo (matériel informatique, mot de passe sur post-it …) sont des indices très utiles pour mener à bien une attaque.

♻️ Fais les mises à jour demandées par les logiciels

- Dans chaque logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées et une mise à jour devra être installé par l'utilisateur.
- Les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations, ne pas procéder rapidement aux mises à jour, c'est rester vulnérable

Cybersécurité n°3 : Virus

☕ Verrouille ton ordinateur lors de ta pause

- Une personne mal intentionnée pourrait profiter de ton ordinateur pour voler des informations confidentielles ou utiliser tes identifiants pour mener une attaque.

💾 Crée des sauvegardes de secours (disque externe / cloud)

- Effectue régulièrement des sauvegardes de secours, permet de récupérer ses données à la suite d'un dysfonctionnement ou d'une attaque.
- Pour sauvegarder tes données, tu peux utiliser un fichier du serveur de ton entreprise ou utiliser disque dur externe.

📪 Crée toi plusieurs adresses e-mail (travail / privé / réseaux / sociaux)

- Les courriels et leurs pièces jointes jouent souvent un rôle central dans les attaques informatiques (courriels frauduleux, pièces jointes piégées...).
- Vous pouvez utiliser une boite mail pour votre vie professionnelle, une boite pour votre vie privée et une boite pour les réseaux sociaux, les jeux, les cartes de fidélités ...

🎁 Méfie-toi des messages inattendus

- Beaucoup de messages inattendus sont en réalité des arnaques ou des tentatives de vol d'informations. Reste prudent et évite de cliquer sur des liens suspects même s'ils proviennent de connaissances !

💳 Pour les paiements en ligne, privilégie les cartes bancaires virtuelles

- Les cartes bancaires virtuelles te permettent de réaliser tes achats sans fournir les informations de ta carte principale.
- N'hésite pas à te rapprocher de ta banque pour connaître et utiliser les moyens sécurisés qu'elle propose.
- De manière générale, ne transmet jamais le code confidentiel de ta carte bancaire.

Cybersécurité n°3 : Virus

MEDIDAS PREVENTIVAS DIGITAIS

Ao adotar as medidas preventivas certas, é possível proteger-se contra ameaças digitais e limitar os impactos de um ataque aos sistemas de informação

Escolher uma palavra-passe muito forte

- Escolha palavra-passe composta, se possível, por 8 carateres de tipos diferentes (maiúsculas, minúsculas, números, carateres especiais)
  Exemplo: ght5CD%7
- Defina uma palavra-passe única e confidencial para cada serviço (banco, mensagens, etc.)

Cuidado ao partilhar fotos e vídeos; estes contêm muitas informações

- Ao partilhar comunicação social nas redes sociais, muitas pessoas vão ter acesso às mesmas.
- As informações visíveis na foto (material informático, palavras-passe em notas, etc.) são pistas muito úteis para levar a cabo um ataque.

Fais les mises à jour demandées par les logiciels

- Em todos os softwares ou aplicações, existem vulnerabilidades. Uma vez descobertas, são corrigidas, sendo depois requerido ao utilizador que instale uma atualização.
- Os atacantes exploram estas vulnerabilidades para levar a cabo as suas operações, pelo que deixar de atualizar rapidamente significa permanecer vulnerável.

Cybersécurité n°3 : Virus

☕ Bloquear o computador durante as pausas

- Uma pessoa mal-intencionada pode aproveitar-se do seu computador para roubar informação confidencial ou para usar as suas credenciais para realizar um ataque.

📦 Criar backups de salvaguarda (unidade externa/cloud)

- Realize backups regulares de salvaguarda, ajudam a recuperar os seus dados após uma avaria ou um ataque.
- Para fazer o backup dos seus dados, pode usar um ficheiro do servidor da sua empresa ou um disco rígido externo.

📪 Criar diversos endereços de e-mail (trabalho / privado / redes / sociais)

- Os e-mails e os seus anexos desempenham geralmente um papel central nos ataques informáticos (e-mails fraudulentos, anexos...).
- Pode usar uma caixa de e-mail para a sua vida profissional, uma caixa para sua vida privada e uma caixa para as redes sociais, jogos, cartões de fidelização...

🎁 Desconfiar das mensagens inesperadas

- Muitas mensagens inesperadas são, na realidade, ataques ou tentativas de roubo de informação. Seja prudente e evite clicar em links suspeitos, mesmo que sejam provenientes de conhecidos!

💳 Para os pagamentos online, prefirir os cartões bancários virtuais

- Os cartões bancários virtuais permitem fazer compras sem fornecer as informações do seu cartão principal.

- Não hesite em contactar o seu banco se informar e utilizar os meios seguros disponíveis.
- De maneira geral, não transmita nunca o código confidencial do seu cartão bancário.

Cybersécurité n°3 : Virus

PRÄVENTION IM DIGITALBEREICH

Die richtige Prävention im Digitalbereich ermöglicht, sich vor digitalen Bedrohungen zu schützen und die Folgen eines Angriffs auf Informationssysteme zu begrenzen.

Ein äußerst sicheres Passwort wählen

- Wähle nach Möglichkeit Passwörter mit acht verschiedenen Zeichenarten (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen).
  Beispiel: ght5CD%7
- Lege für sensible Dienste wie Online-Banking, E-Mail usw. jeweils ein einmaliges Passwort fest.

Sei vorsichtig beim Teilen von Fotos und Videos – diese enthalten sehr viele Informationen

- Wenn Medien über soziale Netzwerke geteilt werden, haben darauf sehr viele Menschen Zugriff.
- Auf Fotos sichtbare Informationen wie Computer-Hardware, Passwörter auf Haftnotizen usw. bieten eine hervorragende Ausgangsbasis für erfolgreiche Angriffe.

Nimm die verlangten Aktualisierungen deiner Software vor

- Jede Software oder Anwendung weist Schwachstellen auf. Werden diese entdeckt, müssen von den Benutzern Patches und Aktualisierungen installiert werden.
- Angreifer nutzen diese Schwachstellen aus, um ihre Angriffe auszuführen. Erfolgen die Aktualisierungen nicht unverzüglich, bleibt die Schwachstelle erhalten.

Cybersécurité n°3 : Virus

☕ Sperre deinen Computer, wenn du Pause machst

- Böswillige Personen könnten von deinem Computer vertrauliche Informationen stehlen oder deinen Benutzernamen für Angriffe missbrauchen.

📦 Mache Back-ups (externe Festplatte/Cloud)

- Wer regelmäßig Back-ups macht, kann seine Daten bei einer Störung oder einem Angriff wiederherstellen.
- Für die Sicherung deiner Daten kannst du eine Datei auf dem Server deines Unternehmens oder eine externe Festplatte verwenden.

📪 Lege dir mehrere E-Mail-Adressen an (beruflich/privat/soziale Netzwerke)

- E-Mails und ihre Anhänge sind häufig Ausgangsbasis für Cyberangriffe (betrügerische E-Mails, virenverseuchte Anhänge usw.).
- Beispielsweise kannst du jeweils ein E-Mail-Konto für berufliche und private Zwecke sowie für soziale Netzwerke, Spiele, Treuekarten usw. verwenden.

🎁 Vorsicht bei unerwünschten E-Mail-Nachrichten

- Viele unerwünschte Nachrichten sind in Wirklichkeit Betrug oder sollen Informationen stehlen. Bleibe vorsichtig und klicke nicht auf verdächtige Links, auch wenn sie von bekannten Personen stammen!

💳 Verwende bei Online-Zahlungen vorzugsweise virtuelle Bankkarten

- Virtuelle Bankkarten ermöglichen dir Einkäufe, ohne die Angaben auf deiner Hauptkarte preiszugeben.
- Erkundige dich bei deiner Bank, welche sicheren Zahlungsmittel sie anbietet.
- Generell gilt, dass der PIN-Code deiner Bankkarte niemals weitergegeben werden darf.

Cybersécurité n°3 : Virus

IFSB

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

CHAMBRE DES METIERS Luxembourg