Devenir un pare-feu humain

Les cinq caractéristiques d'un pare-feu humain

La sécurité de notre organisation dépend de vous, notre pare-feu humain. Vous contribuez à prévenir les incidents compromettant la sécurité et à contrôler l'entrée et la sortie des renseignements sensibles en démontrant ces cinq caractéristiques.

Caractéristique 1 : réfléchir avant de cliquer

Les attaques d'hameçonnage restent la principale stratégie de tout cybercriminel. Les cybercriminels inondent les organisations de courriels contenant des documents et des liens malveillants, sachant qu'il ne suffit que d'un seul clic pour que leur stratagème fonctionne. Les attaques génériques sont faciles à repérer grâce aux fautes de grammaire, aux erreurs d'orthographe ou aux phrases maladroites. D'autres utilisent une approche plus sophistiquée, comme dans le cas de tentatives d'hameçonnage ciblé qui visent des personnes ou des organisations particulières. ***Un pare-feu humain lit ses courriels attentivement, passe son curseur par-dessus les liens pour afficher les adresses URL complètes et traite toutes les demandes de données sensibles avec scepticisme.***

Caractéristique 2 : prendre conscience de la situation

La conscience situationnelle signifie de faire preuve de vigilance, de rester alerte et de ne jamais faire de suppositions. ***Par exemple, si vous voyez une personne inconnue dans une zone normalement réservée au personnel autorisé ou si vous remarquez qu'une porte donnant accès à une zone sécurisée est ouverte, n'ignorez pas la situation! Gardez votre bureau en ordre pour ne pas perdre de documents sensibles et déchiquetez ces documents lorsque vous n'en avez plus besoin. Lorsque vous vous déplacez ou lorsque vous travaillez à distance, gardez un œil sur vos effets personnels, restez à l'affût des épieurs et faites preuve de discrétion lorsque vous accédez à des renseignements de nature très sensible ou lorsque vous discutez de ces renseignements en public.*** Ces comportements non techniques de base sont ceux d'un pare-feu humain très efficace.

Caractéristique 3 : respecter l'accès privilégié

L'accès comprend aussi bien les données de connexion que les badges et les cartes-clés qui vous permettent d'entrer dans des zones sécurisées. Respecter l'accès signifie de veiller à ce que l'autorisation qui vous a été accordée ne soit pas utilisée à mauvais escient, pour quelque raison que ce soit. ***Cela signifie de fermer et de verrouiller les portes, de prévenir le talonnage (lorsqu'une personne se faufile derrière vous à votre insu), de ne jamais divulguer vos données de connexion à quiconque, de verrouiller votre poste de travail lorsque vous ne l'utilisez pas et d'utiliser des mots de passe uniques et forts pour chaque compte et chaque appareil.***

Caractéristique 4 : signaler les incidents immédiatement

Les incidents se produisent. Les signaler immédiatement est la seule manière d'atténuer les dommages et de réduire les risques futurs. Le degré d'importance des incidents n'importe pas. Qu'il s'agisse d'une porte donnant accès à une zone sécurisée laissée ouverte, d'une personne inconnue se trouvant dans le bureau, d'un courriel d'hameçonnage, d'un appareil intelligent ou d'un ordinateur qui ne fonctionne pas correctement, nous comptons sur des pare-feux humains efficaces comme vous pour nous informer le plus rapidement possible, lorsque des incidents comme ceux-ci se produisent. Si vous voyez ou entendez quelque chose d'inhabituel, dites-le!

Caractéristique 5 : toujours suivre les politiques

Les pare-feux humains suivent toujours les politiques de notre organisation et ne les contournent jamais, peu importe la raison. Pourquoi est-ce aussi important? Parce que les politiques définissent notre culture de sécurité. Elles établissent les normes quant à la manière dont les données sont recueillies, stockées, transférées et supprimées lorsqu'elles ne sont plus nécessaires. Elles ont été mises en place pour assurer l'intégrité des renseignements de nos employés, de nos clients, de nos consommateurs et de nos partenaires. ***Le non-respect des politiques peut entraîner des atteintes à la protection des données, des attaques de rançongiciels et d'autres incidents de sécurité néfastes.*** Et même si nous vous demandons de connaître et de suivre nos politiques en tout temps, nous vous encourageons également à poser des questions lorsque vous n'êtes pas certain de quelque chose.