Outlook

Security advice. - conseils de sécurité

De CambridgeGmailbox Louise <cbmailbox08@gmail.com>
Date Sam 2024-10-19 12:30
À Residents Cambridge G <cambridgeg@googlegroups.com>

Dear members / Chers membres

For your information / Pour votre information

Scammers are always on the lookout for opportunities to take advantage of generous but less cautious individuals during calls or messages. These unscrupulous people will exploit your generosity for their own gain at your expense. Be particularly vigilant during this time.
The aftermath of Hurricanes Helen and Milton has left many people without resources, relying solely on government and non-governmental aid, such as FEMA. You may receive solicitations during this period, especially as the holiday season approaches. We recommend reading the following safety tips: it's better to be safe than sorry.

It's well known that scammers often pose as bank representatives. Here's what you should watch out for:

1. **Caller ID Can Be Spoofed**: Don't always trust the caller ID; scammers can fake a phone number to appear legitimate.
2. **We Won't Ask for Your One-Time Verification Code**: We will never call you to ask for your 6-digit one-time verification code. Always read messages in full and follow their instructions.
3. **No Secret Investigations**: We will never ask you to assist with a secret investigation, nor will we request that you transfer funds from your account to "secure" them.
4. **Verify Suspicious Calls**: If you doubt the legitimacy of a call, hang up immediately and call your financial institution using the number on the back of your credit or debit card.

Tips to Protect Yourself from Scams:

- **Never Share Personal Information**: Do not disclose personal or financial information, including PINs and passwords.
- **Verify Caller Identity**: Check the identity of a caller by dialing a trusted number associated with the financial institution or company.
- **Be Cautious of Urgent Requests**: Scammers often create a sense of urgency to make you panic and rush into risky decisions.
- **Beware of Access Requests**: Be suspicious of requests for access to your computer or mobile device (e.g., call forwarding).
- **********

Les fraudeurs sont toujours à l'affût d'opportunités pour prendre avantage de personnes généreuses mais pas suffisamment prudentes lors d'appels ou de messages. Ces personnes, sans scrupules, profiteront de votre générosité pour s'enrichir, à vos dépens. Soyez particulièrement vigilants ces

temps-ci. En effet, les catastrophes consécutives des Ouragan Helen et Milton ont balayé de leurs avoirs beaucoup de monde qui se retrouvent sans ressources outre les ressources gouvernementales et non gouvernementales comme FEMA. Il est possible que vous soyez sollicités ces temps-ci et aussi à l'approche de la Période des Fêtes. Nous vous suggérons de lire les conseils de sécurité suivants. Il vaut mieux prévenir que guérir.

C'est bien connu, les fraudeurs se font passer pour des représentants de banques. Voici ce à quoi vous devez prêter attention :

1 **Ne vous fiez pas toujours à l'identification de l'appelant** : les fraudeurs peuvent usurper un numéro de téléphone pour donner un air légitime à l'appel.
2 **Nous ne vous appellerons pas pour vous demander de nous communiquer votre code de vérification** à usage unique à 6 chiffres. Lorsque vous recevez un code, lisez toujours le message en entier et suivez-en les instructions.
3 **Nous ne vous demanderons jamais de nous aider** dans le cadre d'une enquête secrète, tout comme nous ne vous demanderons jamais de virer des fonds de votre compte afin d'en assurer la sécurité.

4 **Si vous doutez de la légitimité d'un appel,** raccrochez immédiatement et appelez votre institution financière au numéro figurant au dos de votre carte de crédit ou de débit.

Conseils pour se protéger des escroqueries :

1. **Ne divulguez jamais vos renseignements personnels ou financiers**, y compris vos numéros d'identification personnels (NIP) et vos mots de passe.

2. **Vérifiez l'identité d'un appelant** en composant un numéro fiable affilié à l'institution financière ou à l'entreprise en qui vous pouvez avoir confiance.

3. **Faites preuve de prudence** à l'égard des demandes urgentes : il s'agit d'une stratégie utilisée par les fraudeurs pour vous faire paniquer et vous précipiter à prendre des décisions risquées.

4. **Méfiez-vous des demandes d'accès** à votre ordinateur ou à votre appareil mobile (p. ex., renvoi d'appel)

Stéphane Dumas, president

Cambridge G condo association
--