Centro Europeo del Consumidor España

ECC-Net

Cofinanciado por la Unión Europea

GOBIERNO DE ESPAÑA MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

Information note

ECC-Spain warns of suspected identity theft

Some consumers are receiving e-mails from info@register.swanconsultingpro.com posing as the European Consumer Centre.

Madrid, 11 April 2024. The European Consumer Centre in ECC-Spain (ECC-Spain) warns that some consumers are receiving e-mails from info@register.swanconsultingpro.com with the subject line "European Consumer Centre" alerting consumers that they may have been victims of an alleged scam by the company EXTEOM and offering them help to recover the money they have supposedly invested through EXTEOM. ECC-Spain warns that these cases could be identity theft and consumers could be victims of phishing.

ECC-Spain clarifies:
1. ECC-Spain is not forwarding any EXTEOM-related e-mails to consumers.
2. The contact e-mail address of ECC-Spain is cec@consumo.gob.es.
3. Complaints addressed to ECC-Spain are handled through the web form available in its web page https://cec.consumo.gob.es.
4. ECC-Spain complaints are identified with a file number in the following format: ECCES-XXX.
5. ECC-Spain never asks users for security codes.
6. The Comisión Nacional del Mercado de Valores (CNMV) warned in April 2023 that WWW.EXTEOM.COM/ES/ is not not authorised to provide the investment services detailed in Article 125 of the Spanish Securities Markets and Investment Services Act, nor to provide the auxiliary services detailed in Article 126 (a), (b), (d), (f) and (g) of said Act in relation to the financial instruments detailed in Article 2 of said Act, including, for those purposes, foreign currency transactions. For any queries, the CNMV offers users the telephone number 900 535 015 or the CNMV website (www.cnmv.es).

What is phishing?

Phishing is a technique used by cybercriminals to obtain confidential information such as passwords, credit card numbers and other personal information from users. It is also used to install malicious software, malware, on users' devices. To do so, they circulate fraudulent e-mails impersonating the identity of companies and organisations in which the user is asked to access a link provided in the message itself or to download a malicious file. In short, cybercriminals send users messages impersonating a legitimate entity of an organisation to trick and manipulate them into performing some action that endangers their data or installing malware that will capture and send credentials or information when accessing certain pages.

Recommendations to avoid becoming a victim of phishing

- ✓ Do not open unsolicited emails or emails from unknown users. Delete them and block the sender.
- ✓ Do not reply to these emails under any circumstances, nor send personal information such as passwords, personal and bank details.
- ✓ Update all your devices and programs.
- ✓ Verify who is sending you a message before providing any confidential information, even if the message appears to come from a known user.
- ✓ Do not click on links provided in emails without first verifying which website they redirect you to.
- ✓ Do not download any attachments that may be contained in the message.
- ✓ Use up-to-date security software, such as antivirus software.
- ✓ Activate two-factor authentication whenever an online service allows it.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Innovation Council and Small and Medium-sized Enterprises Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible for them.