

# COVID-19-Related Phone Scams and Phishing Attacks

CDC has become aware that members of the general public are receiving calls appearing to originate from CDC through caller ID, or they are receiving scammer voice mail messages saying the caller is from the Centers for Disease Control and Prevention (CDC). Some calls are requesting donations.

<https://www.cdc.gov/media/phishing.html>

It is critical to stay vigilant and follow good security practices to help reduce the likelihood of falling victim to phishing attacks.

- Don't open unsolicited email from people you don't know.
- Be wary of third-party sources spreading information about COVID-19. Refer to the official [CDC.gov](https://www.cdc.gov) website for updates on COVID-19.
- Hover your mouse over links to see where they lead.
- Do not click links in emails. If you think the address is correct, retype it in a browser window.
- Be wary of attachments in any email.
- Do not supply any personal information, especially passwords, to anyone via email

Recently, my colleague received a call asking if he has been vaccinated.

If he is vaccinated, press 1; If he is not vaccinated, press 2.

He pressed 1, As a result, his phone was blocked, and his frequently used payment info and online banking information was transferred.

Everyone, be careful!

Only by clicking, following their instructions, within 3 seconds, they get access to all your bank account information, they disable your phone, and their phone is now controlling your phone number. When they withdraw money from your bank, they will receive the security code (sent to your phone number).

So please look at the caller ID before answering your phone. If it's an unknown number, DO NOT accept the call or do not click on anything.

## Cảnh báo: KHÔNG TRẢ LỜI số điện thoại LA

Tôi nhận được một cú ĐT hỏi tôi đã được tiêm phòng chưa. Nó bảo:

- nếu đã tiêm phòng, hãy nhấn phím 1;
- Nếu chưa tiêm phòng, nhấn phím 2.

**Kết quả là**

- nếu nhấn phím 1, điện thoại bị chặn, và **thông tin ngân hàng của mình đều bị chúng lấy cắp**

Chỉ trong 3 giây nó lấy hết thông tin ngân hàng của mình, nó vô hiệu hoá điện thoại mình. **Khi nó rút tiền, ngân hàng nhắn mã vào số đt của mình nhưng nó nhận được, vì máy mình đã bị vô hiệu hoá.**

**Nên Nhớ : Nhìn caller ID trước khi bắt điện thoại, số lạ khg bắt.  
Lỡ bắt thì gác liền phone, khg nghe, khg trả lời**