Beware of Instagram Scams [1]

Trust Your Instinct

Giveaways, job opportunities, and other scams may skew your judgment. If a post or message seems odd or suspicious, simply ignore or delete it. If it is from someone you know, call the person on the phone to confirm if they really sent it.

While these recent scams appear on the Instagram social media platform, fraudsters will use any method available to scam or phish you out of money or personal and financial information including email at home or work, text messages, voicemail, social media, and gaming apps. Be familiar with the tactics used in phishing scams:

Play on emotions. Messages are often written to generate emotions that will motivate you to take immediately action; fraudsters do not want you to take time to consider the message's legitimacy. The most common emotions include a sense of fear or urgency, or an award of good fortune—something that is too good to be true.

Fake, malicious links and attachments. Fraudsters can use links and attachments to deliver malware—malicious software—to your computer and possibly gain access to CU networks and sensitive work information. Such access may also allow them to lock your computer for ransom until a payment is received. Malicious links can be disguised to look like trusted links and take you to fake or infected websites. Attachments can appear to come from a known source, but whose account has been compromised.

Fraudulent data entry. You are prompted to fill in sensitive information like user names, passwords, and financial information.

Impersonation of individuals or companies. By impersonating an individual or company or both, fraudsters can send phishing messages that look legitimate. They use compromised email accounts and addresses to send the phish. To appear more authentic, business logos are often copied from the Internet and added to the message.

If you have fallen for an Instagram or any other online scam, take steps to minimize the damage:

- Check your bank accounts and credit cards
- Change your passwords.
- Use unique passwords for every online account.

Learn more

- Fight the Phish [2]
- Phishing Scams FAQs [3]

Groups audience:
Office of Information Security
Sub Title:

Students have reported receiving scams targeting their Instagram accounts. The scams focus on obtaining money through gift cards and prepaid credit cards.

Source URL:https://www.cu.edu/security/beware-instagram-scams

Links
[1] https://www.cu.edu/security/beware-instagram-scams [2] https://www.cu.edu/security/fight-phish
[3] https://www.cu.edu/security/awareness/phishing-scams-faqs