Protecting Against Phishing Emails

These days, phishing attacks have been on the rise and at IVCC we do our best to protect your inbox from these email threats – but at times things still can manage to get through.

Here are some warning signs to help you stay vigilant against job offer scams with these red flags:

- Receiving a job offer from an unexpected source.
- Suspicious or misspelled email addresses.
- Unfamiliar or unknown company names.
- Job roles involving money handling or placing orders.
- Requests to print and overnight checks.
- Scammers may send a fake check that will bounce, potentially leading to legal consequences for the recipient.
- Depositing checks on behalf of others.
- Reshipping items.
- Transferring money to unfamiliar accounts.
- Purchasing gift cards or converting cash into Bitcoin.
- Use of your bank account or opening new ones.
- Offers that seem too good to be true.

Exercise Caution: *Scammers may impersonate personnel from IVCC, such as professors or supervisors. Always be cautious when receiving unsolicited job offers from IVCC. Be aware of with text messages claiming to be from IVCC that are not part of RAVE alerts.*

Recognizing Job Offer Scams

Job offer scams typically follow these patterns:

- Unsolicited job offers, often via email, with no prior application or interview.
- Offers for jobs with unusually attractive conditions (e.g., short hours, high pay, remote work) followed by minimal job details in the interview process.
- Offers to help with your resume or job placement.
- Various scam types, including fake checks, requests to handle money, purchase gift cards, or convert cash into cryptocurrency (e.g., Bitcoin).
- Scam emails use generic salutations like "Dear student," avoiding personalization.
- Job descriptions are often vague or entirely absent.
- Legitimate companies don't offer jobs randomly to large groups of people.
- Reputable companies maintain good language standards in their communication.

What Can You Do?

Take proactive steps to verify job offers:

- Contact the company or sender directly to confirm the offer's legitimacy by looking them up online.
- Research the company online; avoid using contact details from the suspicious email.
- If the offer is from someone at IVCC, look up that person in the IVCC Directory and inquire about the job through a new message (do not reply to the original email).
- Search for a Human Resources contact and call to validate the employment offer. This can also be an opportunity to express your interest in the company and inquire about the application process.

If You Think You're a Victim

If you suspect you've fallen victim to a scam:

- Change passwords for any accounts involved.
- Contact relevant financial institutions.
- Report the incident to IVCC IT
- File a complaint at the Internet Crime Complaint Center (IC3) [https://www.ic3.gov/]
- Be cautious of potential threats or further scams using your identity.