

AVOIDING SCAMS



The US Federal Trade Commission has reported an increase in scams attempting to defraud international students of their money or identity. Please be vigilant in recognizing and responding appropriately to these these situations by reading the tips below.

RECOGNIZING SCAMS:

- Scams will claim they represent a government agency in the United States or your home country.
- They will say you owe money for fees or have committed a legal offense.
- They may demand immediate payment over the phone.
- They may ask you to pay with gift cards or other untrackable currency such as Bitcoin.
- They will attempt to keep you from hanging up.
- They may threaten you with legal action if you do not meet their demands.

PREVENTING SCAMS:

- If you believe a call is a scam hang up immediately.
- Do not pay anyone claiming to represent the government over the phone.
- Do not provide your Social Security Number (SSN) or bank information over the phone.
- Do not carry your Social Security Card on your person. Store it in a safe place.
- You can check your immigration status online with US Citizenship and Immigration Services.
- Only go to official government websites or KCISS for immigration information and forms. Government websites in the United States include “.gov” in the web address and all forms are free.

IF YOU'VE BEEN AFFECTED:

- You can report scams to the US Federal Trade Commission at “[FTC.gov/Complaint](https://www.ftc.gov/complaint)” and to KCISS.
- If your SSN has been compromised, visit the Federal Trade Commission website “[IdentityTheft.gov](https://www.identitytheft.gov)” to find steps that you can take to avoid further harm.
- Document all uses of your SSN not authorized by you, and steps you’ve taken to close accounts opened in your name. Documentation can be presented to the Social Security Administration if a major breach of your security is established. You may choose to file a police report as further documentation, but police departments may not be able to investigate fraud.
- Contact the fraud department of any company where you suspect fraudulent use of your SSN and notify them of the fraud. Follow their guidance on changing login information.