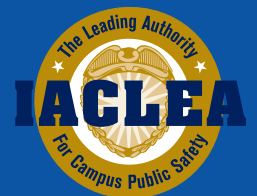
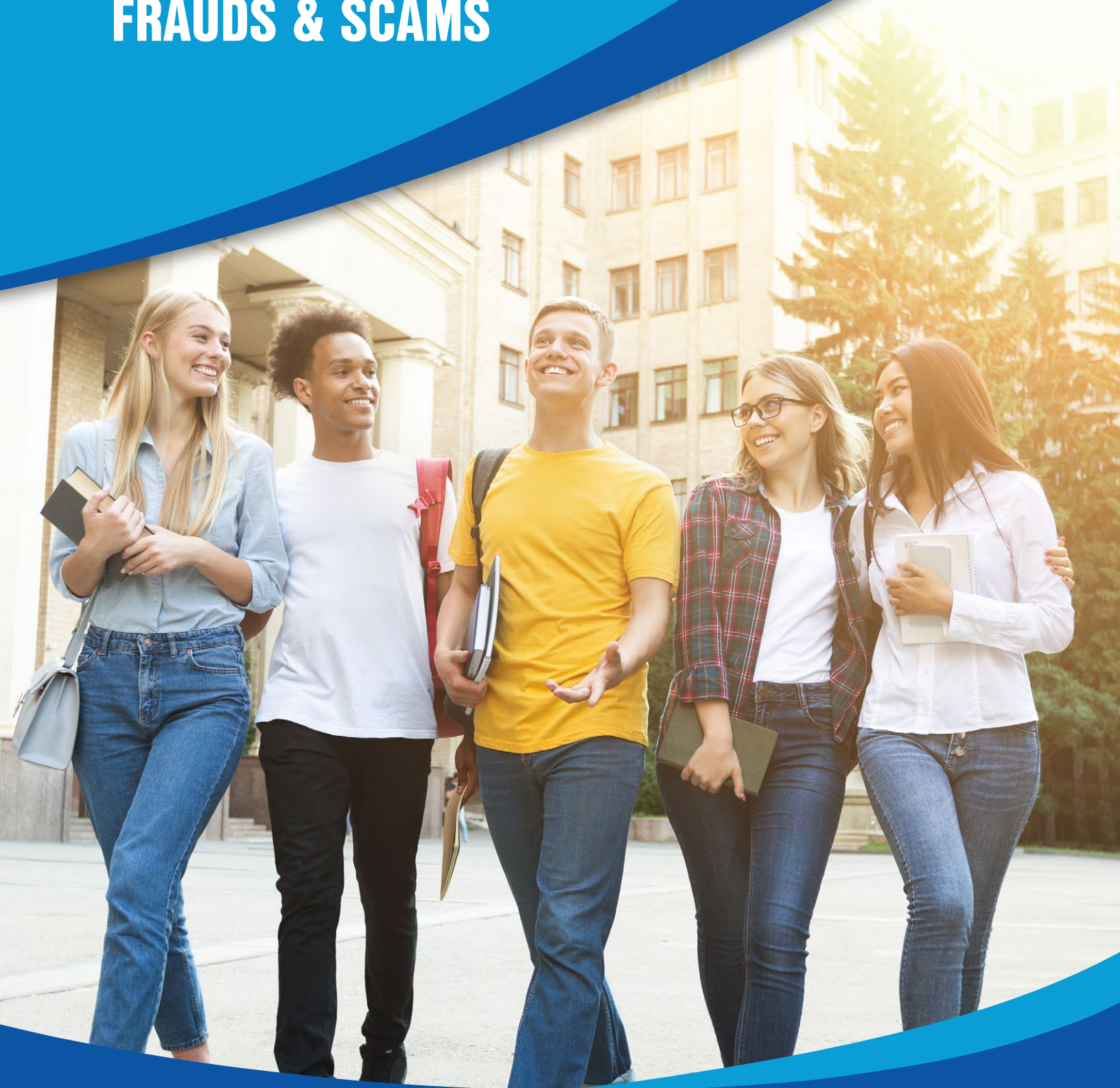


Students Guide

FRAUDS & SCAMS



Students Guide: Frauds & Scams

TABLE OF CONTENTS

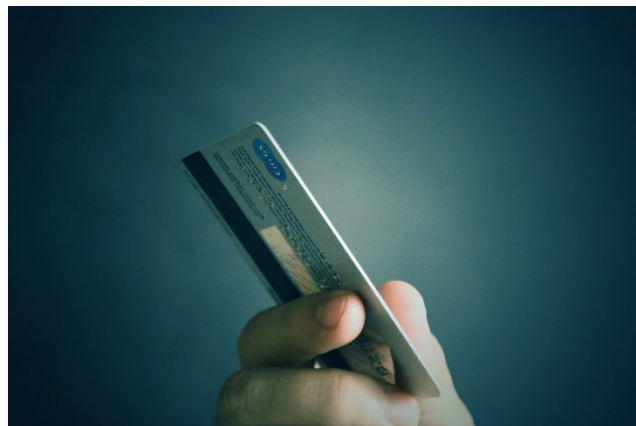
Types of Scams

- 1 Debit Card Scam — Crackin’ Cards.....3
- 2 Student Tax Scams..... 4-5
- 3 Tech Support Scams 6-7
- 4 Instagram Scam.....8
- 5 Student Loan/Scholarship Scams 9-10
- 6 Identity Theft.....11
- 7 Apple/iCloud Scams 12-13
- 8 Amazon Scams.....14
- 9 Behavior Blackmail Scam.....15
- 10 Roommate Rental Scam.....16
- 11 PayPal Scam.....17
- 12 Reshipping Scam18
- 13 Ride Share Scams19
- 14 International Student Scams20
- 15 Peer to Peer Payments (P2P) Payments21
- 16 Fraud Prevention Tips.....22
- 17 Prevention Resources/Guard Your Stash23
- 18 Acknowledgments/Contact Us.....24

1. Debit Card Scam – Crackin’ Cards

What is Crackin’ Cards?

A student opens a new account at a bank, generally with a low dollar amount (\$10-\$25). The student then provides their ATM card and PIN number to a third party. The third party then deposits stolen or counterfeit checks into the account and makes withdrawals prior to the checks being returned as bogus. The student is instructed to tell bank officials they lost their debit card. If questioned how the fraudster obtained the PIN, the student is instructed to inform bank officials they wrote the PIN on a piece of tape and attached it to the back of the card.



Crackin’ Cards Recruitment

Recruiters often resort to social media to recruit students for Crackin’ Cards with the promise of quick money. Here are some examples from social media accounts:

Real Messages Used by Scammers

Walter X
Oct 31 at 4:41PM
This Is Free To Start. If You Don't Have No Money And You Want To Make \$3,500-\$10,000 By Tomorrow All You Need Is An Active Bank Account With Any Nationwide Bank ... To Get Paid.

John P
May 26 at 12:20PM
INSTANT REWARD Instant Money Making Opportunity For All USAA Customers. \$5000K-10,000K Instantly No MONEY NEEDED To Start 100% Guaranteed DM me Now

Jane D
Feb 12 at 11:36AM
ATTENTION if u have an active bank account n trying to make 5k-15k n one day text BANK to 1-555-555-5555* NO MONEY NEEDED!! USAA INSTANT QUALIFY

Mack H
Dec 20 at 12:50AM
ANYONE ONLINE WITH A ... USAA ACCOUNT I CAN GET YOU PAID 1,500 ON DA SPOT YOUR ACCOUNT WILL NOT CLOSE OR OVERDRAFT MESSAGE ME MORE DETAILS

PREVENTION TIPS

- Never share your debit card or PIN with anyone.
- Never deposit a check or money order from an unknown source into your account.
- Don't be a party to a criminal scheme. It's illegal to defraud a bank.

In recent investigations criminal charges have been brought against students for conspiracy and larceny.

**See guardyourstash.com for prevention videos.*

2. Student Tax Scams

For several years, IRS scams have been affecting individuals across the United States. Tax scams tend to increase around tax season, but recently fraudsters are running this scam year-round. There are a couple different types of “tax” scams. In one scenario, the student is contacted, usually via telephone or email, and are told they have not paid their student tax. They are instructed to wire the unpaid taxes to a designated account. The student tax is usually a nominal fee, often less than \$100.00.

In another scenario, the fraudster informs the student they have a legal order pending against them for unpaid taxes. Payment is required or they will be arrested. The scam works like this:



- ▶ The student receives a phone call from a phone number that appears to have an area code around Washington, DC. Below is a transcribed voicemail from an actual fraudster:

*“I am **** and I am calling regarding an enforcement action executed by US Treasury, intending your serious attention. Ignoring this will be an intentional second attempt to avoid initial appearance before a magistrate judge or a grand jury for a federal criminal offense. My number is (***) ***-****. I repeat (***) ***-****). I advise you to cooperate with us and help us help you. Thank you.”*

- ▶ When the student calls the phone number, the fraudster answers the phone, “Internal Revenue Service”. The fraudster sometimes uses threatening language to get the student to cooperate. The student is told the money needs to be paid immediately. Students are threatened with arrest and possible deportation.

- The scammer will inform the student they can pay their taxes by either purchasing gift cards, completing a wire transfer or by sending cash.
- Some students are convinced to pay the unpaid taxes with cards, such as iTunes, Green Dot, Google Pay and Steam cards. The fraudster requests the student provide them with the numbers printed on the back of the card. This expedites the scam.

PREVENTION TIPS

- Some colleges and universities assign enrolled students a student fee (Tax). Before paying the fee, verify the fee is legit at the Bursars Office.
- The IRS **does not** initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. The IRS initiates most contact through regular mail delivered by the United States Postal Service.
- The IRS will never call you and demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer.
- The IRS will never threaten to bring in local police, immigration officers or other law-enforcement to have you arrested for not paying. The IRS also cannot revoke your driver's license, business licenses or immigration status. Threats like these are common tactics scam artists use to trick victims into buying into their schemes.

3. Tech Support Scams

The fraudster contacts the student to offer technical support service. They target Microsoft Windows users. The fraudster claims to be a Microsoft Tech Support Employee. These calls primarily originate from call centers in India. The fraudster will attempt to get the victim to allow remote access to their computer. After remote access is gained, the fraudster uses confidence tricks involving utilities built into Windows and other software to gain the victims trust and pay for services. The fraudster steals credit card information or persuades the victim to log in to their internet banking center, lying that a secure service is connected, and they cannot see the details to receive a refund.

Operation – These scams rely on social engineering. They use numerous confidence tricks to entice students to install remote desktop

software. Once they have access, they take control of the student’s computer and use several Windows components and utilities to make the student believe the computer has issues that need to be fixed.

Initiation – These support scams begin in a variety of ways. They usually begin with a cold call, associated with a third-party Microsoft or Windows Tech Support. They also advertise on popular search engines like Bing or Google. Some scams have been initiated, via pop-up ads, on infected web

sites instructing students to call a phone number. These pop-ups often resemble error messages as the blue screen of death.

Remote Access – The fraudster instructs the student to download and install a remote access program such as, Team Viewer, LogMeIn, GoToAssist or ConnectWise Control, and provide them with the details required to remote control their computer using that program.



PREVENTION TIPS

- **Never relinquish control of your computer** to a third party unless you know it's the representative of a computer support team you contacted. Scammers can steal your personal information and install malware that is later used to commit identity theft.
- **Be wary of unsolicited calls.** Legitimate tech companies don't make unsolicited calls to their customers. This is a popular scam tactic. Remember, scammers can spoof official looking phone numbers, so don't trust your Caller ID.
- **Look out for warning screens.** Nearly half the tech support scams begin with an alert on the student's computer screen. This pop up will have a phone number to call for help. Instead of calling, shutdown your computer and restart it.
- **Don't click on links in unfamiliar emails.** Scammers also use email to reach students. These messages point consumers to scam websites that launch pop-ups with the fake warnings and phone numbers.
- **Beware of anyone asking for untraceable payments.** Scammers often ask for payment via wire transfer, gift card or pre-paid debit cards. Legitimate companies do not ask to be paid this way.
- **Download software only from official vendor sites or the Microsoft Store.** Be wary of downloading software from third-party sites. These sites may have been modified without the owner's knowledge to bundle support scam malware or other threats.
- **Use Microsoft Edge when browsing the internet.** It blocks known support scam sites using Windows Defender SmartScreen. Never call the number in the pop-ups. Microsoft's errors and warning messages never include a phone number.
- **Enable Windows Defender Antivirus on Windows 10.** It detects and removes known support scam malware.

4. Instagram Scam

Recently, fraudsters have been messaging students via Instagram. The topic of the message is usually of interest to college students, such as “saving money with this new app.” This message will be followed by a link (usually a URL shortened with bit.ly).

Once clicked, this link will authorize a third party to have access to your Instagram account. Fraudsters will now use your account to post advertisements on your profile, message your friends, and comment ads/spam on people’s posts.



PREVENTION TIPS

- ▶ **Do not open messages from unknown users.** If you do not know who the person is, ignore the message. If you see a link you are not familiar with, do not click it.
- ▶ **If you have already clicked the link** and are experiencing suspicious activity, check your authorized applications list. You can do this by logging in on a web browser and going to Edit Profile > Authorized Applications > Remove Unknown App. To be safe, change your password too.

5. Student Loan/Scholarship Scams

Students are being targeted by several scams to include guaranteed scholarships, financial aid and/or offers of student loan debt relief. The scammers prey on the financial needs of the student with the promise of a significant award or lower cost loan. In reality, their goal is to either get the student to pay up-front costs or fees for which the student will receive no benefit, or obtain the student's personal identifiable information (PII), bank account numbers or credit card information.



Scholarships

Many of these scams guarantee a scholarship which is just not true. No scholarship is guaranteed, and the scammers typically ask you for an upfront management, processing or enrollment fee. Once the fee is paid, there are requests for additional fees or there is no further contact with the student from the solicitor. Scholarship applications must be submitted by the student, not a third party. The student must write their own essays and gather their own letters of recommendation. A third party who offers to do all this for you should be a red flag that it's a scam. Another red flag is you receive an email or phone call advising that you have been selected for a scholarship, a scholarship you never applied for. Scammers often use pressure tactics advising the student to act fast or risk losing the scholarship. In reality, they are only trying to get your financial information.



Loans and Debt Relief

In some circumstances scam loan companies will tell you they can get you the best rates, for a nominal fee. Legitimate student loans do not require upfront fees. If there are any processing fees involved, they are lumped into the repayment amount or deducted from the loan disbursement. Loan consolidation scams typically charge students a consolidation fee upfront and then don't deliver on the promise. Student loans can be consolidated for free at <https://studentloans.gov/myDirectLoan/index.action>

Student loan debt elimination is also a well-known scam. Legitimate student loan debt must be repaid and can only be eliminated in rare circumstances for reasons like permanent disability, death or falsified documents.

PREVENTION TIPS

- Ignore offers with a demand for an immediate answer.
- Never give out your personal identifiable information, including your Social Security number, bank account numbers or credit card information.
- Never share your FSA ID or sign a power of attorney or third party authorization allowing someone to act on your behalf relative to your student loan.
- Do not pay a third party to manage and make payments for you.
- Verify the existence of the business, via directory assistance and the internet.
- Visit the US Department of Education Federal Aid website at <https://studentaid.ed.gov/sa/repay-loans/avoiding-loan-scams>. This website has a lot of information regarding seeking help from trusted debt relief companies and actions to take if you've already shared personal information with a student loan debt relief company.
- Ignore a company that claims they are affiliated with the Department of Education.

6. Identity Theft

Identity Theft occurs when a fraudster steals key pieces of your personal identifying information (PII) and uses this information to gain access to your financial and personal accounts, open new credit and/or financial accounts, purchase vehicles, rent apartments, open utility accounts, phone services, etc. PII may include your name, date of birth, Social Security number and mother's maiden name.



Monitor Your Credit:

1. Review credit card and financial account statements each month and reconcile purchases.
2. Order your free Consumer Credit Report each year and review the report for accuracy. You can order the free credit report online at annualcreditreport.com.
3. If you are concerned about becoming a potential victim of identity theft you can freeze your consumer credit file by contacting the 3 Credit Reporting Agencies, via their websites. Click on the tab for credit freeze. This will make it extremely difficult for a fraudster to open new accounts using your identity.

TIPS TO PROTECT YOUR IDENTITY:

- Never give PII over the phone or internet unless you initiated the contact.
- Never input your credit card or financial account information at a website unless it offers a secure transaction. Indications of a secure transaction include an icon of a lock at the bottom strip of the web browser page. The URL address for the webpage will change from "http" to "https".
- Shred unwanted important documents containing PII before discarding them.
- Memorize your Social Security number. **Do not** carry your Social Security card in your wallet or purse.

7. Apple/iCloud Scams

Students will often receive phone calls and emails impersonating Apple in attempt to retrieve their personal identifiable information (PII), bank account numbers or credit card information.



Fake Phone Calls:

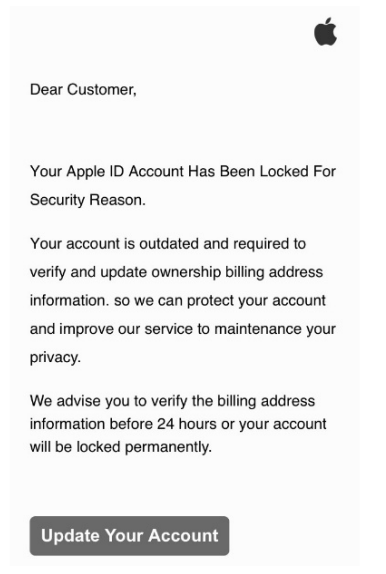
Fraudsters will call impersonating Apple technical support. Like Microsoft scams, these calls primarily originate from call centers in India. They will claim someone tried to login to your Apple ID/iCloud or they have detected suspicious activity on your account. For them to resolve the issue, the fraudster requests for your name, email, phone number, password, and other PII.

PREVENTION TIPS

- **Be wary of unsolicited calls.** Apple support will never call you unexpectedly – only when you have initiated contact with them first.
- **Legitimate companies will never ask for your password.** Even if you are on the phone with real Apple support, they will never ask for passwords.
- **Scammers are persistent** and will pressure you for information claiming it is necessary. Real tech support representatives will not attempt to persuade you for PII. Scammers will also consistently call you back if they feel you are vulnerable to their tricks.
- **Legitimate tech representatives should know your name.** Once you have initiated contact with Apple support, they will address you by the name you provided when requesting a call back.
 - **Example:** “Hi this Jean from Apple, am I speaking with John?”

Fake Apple Emails:

Fraudsters are aware that most students use Apple and iCloud. They will often send students realistic looking (but fake) phishing emails. Here are some real examples of these emails:



Dear Customer,

Your Apple ID Account Has Been Locked For Security Reason.

Your account is outdated and required to verify and update ownership billing address information. so we can protect your account and improve our service to maintenance your privacy.

We advise you to verify the billing address information before 24 hours or your account will be locked permanently.

[Update Your Account](#)

Apple Thursday >
RE: [ALERT] Someone has accessed your acco...
Update your Account Informations! Dear Client,
We have faced some problems with your acco...

Apple ID 10/15/19 >
RE: (ALERT!):[More Information Update] We'v...
YOUR APPLE ID HAS BEEN LOCKED
Your Apple ID was used to sign in to App Store...

Apple 10/15/19 >
Re: [Daily Email Report] [Fraud Activity Statem...
AStatement Update October, 15 2019
PDTpJLVFILQZERpJLVFILQZERIJLVFILQZEReb...

Fraudsters can easily fake the sender email address. For example, the email can appear that it is from "Apple," but is really from hfn3an3ggt@awalannew25.com. More advanced fraudsters can spoof sender email addresses so they appear to be from support@apple.com or other legitimate emails. Clicking "Reply" will reveal the real full email address of the sender.

The fraudulent emails usually claim someone unauthorized has accessed your account or that your Apple ID/iCloud has been locked for security purposes. Once opening the email, there will be a link for you to click to "Update/Verify your account" or a PDF/DOC file for you to download with "more information." Do not click/download as this is their way of stealing your personal information or granting the attacker with remote access to your device.

PREVENTION TIPS

- **Legitimate companies will never refer to you as "User" or "Customer."** Apple and other companies will always address you by the name listed on your account.
- **Clicking "Reply" will reveal the real email address of the sender.** Fraudsters have tactics to make the sender email address look real.
- **Fake emails will often contain spelling errors.** This is an easy way to determine if the email is fake.

8. Amazon Scams

Like Apple scams, fraudsters will call and email students impersonating Amazon in attempt to collect their credentials and PII.



Fake Phone Calls:

You may receive a call from an automated voice recording alerting you that a large purchase was made on your Amazon account. To resolve this matter, you are asked to dial "1" to be connected to Amazon technical support. Once connected, the fraudster will ask you for your name, phone number, credit card information, passwords, etc. Amazon will never call you unless you have initiated contact first or ask for your passwords and credit card information.

Fake Amazon Emails:

Amazon generally contacts customers via email. Fraudsters attempt to trick students by sending out phishing emails imitating Amazon support. These emails will claim there was a billing problem or a suspicious login on your account.

Click "Reply" to reveal the real sender email address. Do not click the links provided in the email or download the document files – this is their way to phish you or remote control your device.

Here is an example of a fake Amazon email. Notice how clicking on the "From" email revealed the real sender email address.

The screenshot shows a mobile email interface. On the left is a contact card for "customer-support@amazon.com" with a grey circular profile picture containing a white letter 'C'. Below the name are four icons: a blue speech bubble for "message", a grey telephone for "call", a grey video camera for "video", and a blue envelope for "mail". Below the contact card, the text "other" is followed by the email address "email.amazon-customer3527@obehabatuk...".

On the right is an email preview. The "From" field shows "customer-support@amazon..." with a grey circular profile picture containing a white letter 'C'. The "To" field is redacted with a black bar and has a "Hide" link. The subject line is "Re: [Statement Update is available] : Information notice Your Activity Account Submitted Changed to Your Billing Information on October 14 2019 / [Relevé de compte] Votre paiement a été programmé: [41465780](#) l'achat de votre reçu de transaction sera". The date and time are "October 14, 2019 at 7:20 PM".

Below the email preview is a PDF attachment icon with the text "Amazon Pa...Service.pdf" and "56.4 KB".

9. Behavior Blackmail Scam

College students are extorted for money in return for maintaining their reputation on campus, with family and friends. Students are caught on video doing something inappropriate or share intimate photos. The blackmailer threatens to publish the unsavory video or photographs on social media unless payment is made immediately.

Students have hooked up on dating sites and convinced to send their “match” intimate photos. Once that’s done, the match will demand additional compromising photos and/or sexual favors

from the student. If the student is uncooperative, the match will threaten to post/share the photos across social media platforms, via email or through other online dissemination.

Others have been tricked into sending intimate photos to someone impersonating a celebrity, talent scout, singer or athlete. Once that’s done, the impersonator will blackmail the sender and demand money, sexual favors, more intimate photos or videos. The perpetrator gets a rush from the control they hold over the student.

Behavior blackmail has serious consequences and can have devastating outcomes. Some cases have resulted in students taking their own lives. Other matters have resulted in serious criminal charges filed against those who have posted photos of students, who were minors.



PREVENTION TIPS:

- With the prevalence of a phone in every hand and a multitude of social media apps, students should be aware their every action can make its way to the internet with the click of a button.
- Keep apps and privacy settings set to the strictest levels possible.
- Do not share compromising photos with anyone, even dating partners. Not all relationships last forever or end on amicable terms. Do not save intimate photos on your device.
- Be mindful of others who may be impaired and acting inappropriately – be respectful and don’t take or post pictures of them online. The internet is forever and a lapse in judgment today can come back to haunt you in the future.

10. Roommate Rental Scam

This scam is one of many variations of fake check scams. The fraudster answers an ad online or through a phone number posted on campus claiming to be a potential roommate. The fraudster sends a check in an amount that exceeds the agreed upon initial rent. The check is deposited into the bank and appears to clear. The funds are credited to the account. The potential roommate (Fraudster) requests the extra money, an amount paid above the agreed upon price, be returned to him/her via wire transfer, through a digital financial transaction such as Venmo, Apple Pay, etc. or via Mobile Deposit if the account holder provided log on credentials. The excess money is returned to the potential roommate (Fraudster). On a later date the bank notifies the student the deposited check is bogus and the student is out the money.



A variation of the Roommate Rental Scam is when a student answers an ad online. The ad includes photos of the apartment and requested rent. The fraudster claims to be out of town and is unable to show the unit. A refundable deposit is requested to hold the unit until he/she can show you the apartment. The deposit is electronically remitted to the fraudster. The fraudster never owned the unit and the student is out the money (Deposit).

STUDENT PREVENTION TIPS

- Trust your gut – If the apartment seems too good to be true, it probably is.
- Beware of a roommate or landlord who can't meet with you in person. If your only way to communicate with them is via email, be very wary.
- If you're pressured into sending a deposit immediately, slow things down until you can properly research the offer.
- Do your research on the apartment and the people. Always be skeptical.
- Search "Roommate Scams" online to learn about the most recent scams.

11. PayPal Scams

PayPal typically uses email to contact its customers. The information below can help you make sure it's really PayPal, and not somebody trying to gain access to your account.



Fake email addresses:

Fraudsters can easily fake the PayPal name in the sender's email address. For example, an email can appear to be from "PayPal Services," but is actually from `spfr2013qz7@nomail.com`.

If you mouse over the name or click "Reply," you should be able to see the full email address of the sender. Sophisticated fraudsters can fake the entire name to look like a legitimate sender, so be careful.



If you do click a link in an email, be sure to review the URL of the site where you land. It is easy for bad guys to copy the look of a legitimate website, so you need to check that you are at the correct website.

An email from PayPal won't:

- Ask you for sensitive information like your password, bank account, or credit card.
- Contain any attachments or ask you to download or install any software.

PREVENTION TIPS

- Don't give out personal information to a person or company you don't know.
- Be suspicious of any offer that doesn't pay a regular salary or involves working for an overseas company.
- Check the company with the FTC, Better Business Bureau, or state Attorney General.

VERIFY THROUGH YOUR PAYPAL ACCOUNT:

- If you receive an email that says that you've received a PayPal payment, take a moment to log in to your PayPal account before you ship any merchandise. Make sure the money has actually been transferred, and that it isn't a scam.

12. Re-Shipping Scam

Most re-shipping scams originate when a student answers an on-line advertisement, applies for a position on a job board or other official looking website for “work at home” positions.

Successful applicants are promised thousands of dollars for working at home with no special skills and minimal training. These jobs are very attractive to students, stay-at-home parents and seniors.

These positions are often advertised as merchandise managers, import/export specialists or package processing assistants.

The employer (Fraudster) describes the duties of the position to include:

- ▶ Receiving merchandise from merchants (Usually Electronics).
- ▶ Consolidating and repackaging the merchandise.
- ▶ Affixing postage paid mailing labels.
- ▶ Re-shipping parcels to an overseas address.

What most people don't realize is the merchandise was purchased with stolen credit cards or counterfeit checks and you, the employee, are an unwitting co-conspirator to the crime.

Here is an example of what a job ad might look like:

CL

- ★ Feb 27 *****WORK FROM HOME ***** Shipping specialist
- ★ Feb 20 WORK FROM HOME in 2019!!!!!!!
- ★ Feb 13 Shipping Specialist Needed PART TIME WORK FROM HOME
- ★ Feb 13 Make \$1200/WK ***STAY AT HOME***



PREVENTION TIPS:

- ▶ Steer clear of job advertisements where the position description involves repackaging or re-shipping merchandise.
- ▶ Do not provide your personal identifiable information to on-line job applications. Your information may later be used in an ID Theft scheme.
- ▶ If the salary does not match the actual work effort, it's a scam.

13. Ride Share Scams

Whether you are riding with Uber, Lyft, Via, or any of the other Transportation Network Companies (TNC), the most important first step you can take to ensure your ride is seamless and safe is to make sure you enter the right vehicle. Prior to pick-up, every TNC provides the customer with valuable information to ensure they enter the correct vehicle. Information should include the vehicle make and model, the first name of the driver, photo of the driver and the vehicle license plate number. When your driver arrives, politely ask him/her their



name and check their answer against the name provided on the app. Make sure the make and model of the car is accurate and ensure the license plate matches the information provided on the app. If any of the observed details **do not** match those on the app, **do not enter the vehicle**.

Once inside the vehicle, your driver should never ask you to pay in cash. If the driver pressures you to provide cash, ask to exit the vehicle and call 911. If the driver refuses to allow you to exit the vehicle, call 911.

Where you live is an important piece of information and you may not want to share this information with others. Instead of being dropped off directly in front of your apartment, house or dorm, select a drop off location adjacent to your residence.

Most of the time after you exit the vehicle, your payment will be immediately processed. If you notice a cleaning fee charge (\$100-\$300) for no legitimate reason (you did not make a mess or vomit in the vehicle), immediately access the company website, select the trip in question and select the help section. There you will find a link titled "Dispute Cleaning Fees." Click this link and dispute the charge. You should also contact your credit card company and dispute the charge.

If you find an unauthorized charge on your credit card statement, immediately report this information to your local law enforcement agency and your credit card company. Also, some TNC's have an app support for unauthorized transactions. For example, for unauthorized purchases made through Uber, go to: <https://help.uber.com/h/fe547761-4384-42d4-8531-4cfb0e0e523e> and complete the required information. Uber will refund the amount for each unauthorized trip and provide you information linked to the unauthorized transactions such as the phone number and email associated with the account as well as the trip pick up and drop off locations.

14: International Student Scams

- Scammers pretending to be from the federal government are scaring international students into paying them money.
- Foreign students, particularly from South Asian countries, are getting phone calls that look like they're from the government.
- The caller typically knows about a student's immigration status and the program or school they're attending.
- They will say there's a problem with the student's immigration documents or visa renewal. And then they will demand immediate payment, often thousands of dollars, for a fee or bogus immigration bond.
- Callers have made threats, including arrest or deportation, if the students don't pay, and they ask to be paid with gift cards (like Google Play or iTunes) or a cryptocurrency (like Bitcoin).

What are the signs that these are scam calls?

- The federal government wouldn't make such calls, wouldn't make such threats, and wouldn't ask for such payments.
- Any callers who want to be paid with gift cards or cryptocurrency are scammers, who like those payment methods because they can get the money and disappear without a trace.

Scammers also go after international students' money

- If you get a call that's anything like this, hang up the phone.
- If you're not convinced it was a scam, talk to someone you trust about the call. Several people report that they figured out the call was a scam after talking with a relative, the local police, or a school official. It's likely that others in your community got the same call, so talking about the call could help others in your area.
- If you're concerned about your visa or immigration documentation, call USCIS's National Customer Service Center at 800-375-5283.

15: Peer to Peer Payments (P2P Payments)

- Peer to Peer (P2P) apps are designed to simplify financial transactions between people who know and trust each other.
- P2P apps allow users to send money from their mobile devices through a linked bank account or card.
- The use of peer to peer (P2P) mobile payment apps such as CashApp, Venmo, and Zelle is growing.
- Splitting the check at dinner or sending utility bill payment to a roommate are popular uses of P2P apps.
- For the most part, P2P Payments are also secure because they're encrypted and have fraud monitoring capabilities.

As Americans grow more comfortable using these apps, scammers have adapted their tactics to take advantage of the quick and often anonymous access to cash that they provide.

Some steps to help you avoid being scammed when using payment apps:

- Avoid using P2P Payments for goods and services.
- Before donating with a P2P app, always check the charity's website to verify that they accept donations through that app.
- Even a legitimate transaction can go wrong by entering an incorrect phone number or misspelling a recipient's name, resulting in the funds going to the wrong person.
- Always verify the recipient's information before making any payment.
- Never send P2P Payments to – or accept payments from – someone you don't know.
- Have strong passwords and never hand your cell phone to someone you don't know for any reason. Fraudsters can send money from your P2P app to their account within 10 seconds without your knowledge.
- Once the funds are transferred the money is lost forever!!

16: Top Ten Fraud Prevention Tips

1. Get your free credit report at **annualcreditreport.com**. Each year you may receive 1 free credit report from each of the 3 credit reporting agencies (TransUnion, Equifax or Experian). Upon receipt, check for unauthorized accounts, inquiries and unknown addresses.
2. Register to access your Social Security benefits statement at www.ssa.gov. Upon receipt, review your estimated benefits and earnings record. You should also ensure no one is using your Social Security number for employment or other benefits.
3. Know who you are paying, via person to person payments, i.e., Zelle, Venmo, etc. Pay and receive money only with people you know. Don't pay strangers with P2P (Person to Person). Most "person to person" transactions are instantaneous and irreversible.
4. Do not pay for merchandise online or via the phone using a debit card. Debit cards are vulnerable because they are linked to a bank account. You have a far better chance of resolving a fraudulent transaction when paying with a credit card rather than with a debit card. Also do not provide your debit/credit card numbers over the phone, via emails or on websites unless you initiated the call or order.
5. Keep thorough records. If your laptop is stolen, can you provide a full description to the police? Write down your computer's make, model, color and most importantly the unique serial number, which acts as a key identifier, much like the vehicle identification number (VIN) on a car. You might also need this information to file an insurance claim.
6. Do not use an ATM machine if you notice wires or a skimming device attached to where you insert your card. Also, cover the keypad with your hand, a hat or other piece of clothing when inputting pin numbers. Notify the bank or local police if you observe device(s) attached to the ATM.
7. Do not make a debit card purchase without first verifying the account balance. Most financial institutions will allow the transaction to process through even when you don't have enough funds to cover the charge. This will result in penalties and unnecessary fees.
8. Don't assume an email or phone call is authentic. Just because someone knows your basic information (such as your name, date of birth and address), it doesn't mean the email or phone call is legit. Criminals will use a range of social engineering techniques to get your personal identifiable information.
9. When leaving bars or restaurants late at night do not accept a ride from a person who purports to be employed by a well-known private car service or transportation network company unless you initiated the call for service. In the past, fraudsters have driven students to secluded areas and robbed them. In other cases intoxicated customers were driven to ATM machines and forced to withdraw funds from their accounts.
10. Do not offer to deposit a check into your account if requested by an unknown individual. The individual may claim they do not have an account and offer a sob story. You are financially responsible for all Items deposited into your account. Do not provide your account log on credentials to anyone. If you do, they can deposit stolen or counterfeit checks into your account. The bank will hold you financially responsible.

Trust Your Gut – If something just feels wrong, it probably is.

Fraud Prevention Resources

International Association of Financial Crimes Investigators

The **IAFCI**, a non-profit international organization, provides services and an environment within which information about financial fraud, fraud investigations and fraud prevention methods can be collected, exchanged and taught for the common good of law enforcement, the financial payment industry and our global society. **Information on scams can be found on the public website under <https://www.iafci.org>.**

Federal Trade Commission (ftc.gov) - has great information on scams targeting college students. You can go on to their website and sign up for daily alerts.

Visit www.guardyourstash.com/ for information and prevention videos on the debit card scam.

Guard Your Stash

[HOME](#)

[WHAT TO LOOK FOR](#)

[PREVENTION VIDEOS](#)

[CONTACT](#)

Don't Be a Fool

If someone on social media tells you of a **great way** to make money by giving up your debit card and PIN or letting them put a check in your account, **DON'T DO IT**. It's a **SCAM** and you will be left *owing* your bank money, **destroying** your credit for life, along with *criminal charges* and *jail time*.

For more information on the debit card scam and other frauds and scams, go to www.iafci.org

Acknowledgments

- **Phil Bartlett,**
United States Postal Inspection Service
- **Michael Carroll,**
United States Postal Inspection Service
- **Brian O'Connor,**
Cambridge Police Department
- **Missy Coyne,**
NICB
- **Wade Stormer,**
Uber



IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS
1020 SUNCAST LANE, SUITE 102
EL DORADO HILLS, CA 95762

WWW.IAFCI.ORG
TEL. 916-939-5000