Georgia Tech Office of International Education

SCAMS 101

Depending on where you've lived in the past, you may or may not have had to beware of and deal with getting swindled. Scammers are getting increasingly sophisticated in their attempts to get your money or personal details. Here's what it may look like in the USA and how you can handle it.

Ways you can be scammed

Phone Call Scams

What it looks (or sounds) like	What it actually is
Unknown number, may be local	A Potential Scammer or Robocall
Caller ID displays the number of a bank, insurance company, or even the government	Caller ID Spoofing, spoofers can mask the number they're calling from using legitimate numbers
You answer the phone and before you have a chance to say anything a voice begins introducing itself	A Robocall, the voice is a recording and will ask you to hit a button or take certain steps
You answer and the caller introduces themselves as an employee of an agency, they speak quickly, professionally, and assuredly. They may even provide personal identifiable information about you (like your immigration status or where you study/work). They will inform you of a problem and ask you to verify some personal information.	A Potential Scammer, they may have found your information online and speak quickly and with confidence to overwhelm you so that you worry about the issue they mentioned and have little time for suspicion. Common scenarios are explored below.

Common scenarios:

- Calls from the **Internal Revenue System (IRS)** that threaten to have you arrested or deported for owing taxes then proceed to ask for credit/debit card information.
- Calls from the **Social Security Administration (SSA)** that say you're due a cost-of-living increase, or that "SSA computers are down", or may refer to enrollment in the Medicare prescription drug program and then ask you to verify personal information like your SSN.

- **Prize and lottery scams** where the caller will say you've won a prize, but then say you need to pay a registration or shipping fee to get it. But after you pay, you find out there is no prize.
- **Tuition Payment scams** from organizations making false claims to have an affiliation with your university, offer you a tuition discount, a currency exchange discount, or make other promises. This is their attempt to confuse you before they are fully aware of their institution's official payment process.

Emails (Phishing)

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication (usually an email).

What it looks like	What it actually is
An email from someone giving a **very detailed story** of why they **need your help/money** and how it will be an investment and end up benefiting you. They will ask you to reply, then start a dialog with you to gain your trust and seem credible. They might even include a phone number to call if you have questions.	A scammer trying to get your personal information or money, using conversation to gain your trust.
An email about anything (like an advertisement or informing you that you've won a prize) with a **link** either as **hypertext** or an **image**.	A fake link which takes you to a fake website where any information you input isn't safe or which downloads a virus on to your computer.
An email about anything (may even seem professional -work or school related) with **attachments**.	A virus attachment which contains a virus which will then either send your information to the scammers, or allow them to access your computer. The virus may be completely invisible and leave your

	computer performance unaffected, such as a **Keylogger virus** which records your keystrokes and from that, the scammers/hackers can identify frequently typed strokes such as your passwords.

Common scenarios:

- Emails from what appears to be the **provider of a service you use**, such as your bank, asking you to click a link and enter your login and password.
- Emails from a **person of high notoriety**, like a celebrity or governmental figure (sometimes fictional, sometimes real) asking for your help or claiming they wish to help you/invest in something with you. They'll ask if you're interested and to respond or click a link if you are.
- **Scholarship/Honor Society** invitation or acceptance letters. These emails may look professional and use personally identifiable information such as your name and school you attend, and will usually be sent out once last semester's grades are available to increase credibility. They usually link you to a seemingly legitimate website where you input personal information or pay to join the society.

How you can avoid it

Phone Call Scams

Generally:

- If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, you should **just hang up**. Scammers often use this trick to identify potential targets.
- **Do not respond to any questions**, especially those that can be answered with "Yes."
- **Never give out personal information** such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- **Always verify who you are speaking to**:

  If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.
- Use **caution** if you are being **pressured for information immediately**.
- If you have a voicemail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voicemail if you do not set a password.
- Talk to your phone company about call blocking tools they may have and check into apps that you can download to your mobile device to block unwanted calls.

- Report robocallers: If you use robocall-blocking technology already, it often helps to let that company know which numbers are producing unwanted calls so they can help block those calls for you and others.
- To block telemarketing calls, register your number on the Do Not Call List. Legitimate telemarketers consult the list to avoid calling both landline and wireless phone numbers on the list.

Remember: You always have the right to ask the caller to repeat what they said or ask why they want certain information. While the best option is to hang up and call the organization that seemingly called you using the number listed on their website, you could also be skeptical and inquire about what's being asked of you before you answer any questions.

Specifically:

Note that the **IRS** will not:

- Call you to demand immediate payment. The IRS will not call you if you owe taxes without *first sending you a bill in the mail*.
- Demand that you pay taxes and not allow you to question or appeal the amount you owe.
- Require that you pay your taxes a certain way. For instance, require that you pay with a prepaid debit card.
- Ask for your credit or debit card numbers over the phone.
- Threaten to bring in police or other agencies to arrest you for not paying.

If you don't owe taxes, or have no reason to think that you do:

- Do not give out any information. Hang up immediately.
- Contact TIGTA to report the call. Use their "IRS Impersonation Scam Reporting" webpage. You can also call 800-366-4484.
- Report it to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" in the notes.

If you know you owe, or think you may owe tax:

- Call the IRS at 800-829-1040. IRS workers can help you

Note that the **SSA** will not:

- Threaten you.
- Suspend your Social Security number.
- Demand immediate payment from you.
- Require payment by cash, gift card, prepaid debit card, internet currency, or wire transfer.
- Ask for gift card numbers over the phone or to wire or mail cash.
- You should contact the SSA and ask for verification. If the SSA is unable to authenticate the communication you received, you should report it to the SSA Office of Inspector General at 1-800-269-0271 or online at https://oig.ssa.gov/report.

Emails (Phishing)

Generally:

- You should always stop and **think before you click on a link**. Links can be deceiving; hover your mouse over the link and verify that it is taking you where you want to go. If you are viewing the link on a smartphone, holding your thumb on the link should reveal the actual destination of the link. You can also go to your browser and find the destination of the link manually (like accessing your online banking login page by searching for it rather than clicking the link in an email).

- **Do not respond to suspicious emails**, especially those that you receive from persons of high notoriety, they would never contact you directly.

- Beware of **fake websites.** If you do click a link and end up on a website whose URL begins with anything other than "https://" (or if on a browser there is no lock symbol before the URL). **The URL should start with "https://" not "http://".**

- **Never give out personal information** such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected emails or on fake websites.

- **Attachments**: If the email and attachment is from an **unknown source, delete the email** immediately. If the email and attachment

appear to be from a trusted source, but not expected, pick up the phone and call the person to verify if they actually sent you the message.

- **Don't trust any contact information** contained in the email. Navigate to the actual website of the organization in question and obtain their contact information directly from their website.

Specifically:

Note that with regards to Georgia Tech communication:

- 99.5% of all legitimate Georgia Tech websites will have a domain that contains "gatech.edu" (e.g. https://passport**.gatech.edu**).
- High priority/sensitive emails from Georgia Tech should come from emails within the Georgia Tech domain (e.g. comments@registrar**.gatech.edu**). They will also contain the copyrighted Georgia Tech logo.
- Please contact the Office of International Education/ International Student Scholar Services or the Office of Student Integrity prior to responding and/or providing any financial information or funds to determine the legitimacy of any communication which mentions that your standing as a student at Georgia Tech or your immigration status as an international student is at risk (and that the action to be taken involves giving banking/personal information).

Remember: You should never share your login and password with anyone for any reason.

How to deal with getting scammed

Remember: Reporting scams will not affect an international student's immigration application or petition. Also, many states and federal agencies allow students to report scams anonymously.

Identity theft (SSN theft)

Report **identity theft (SSN theft)**:

- To the **Federal Trade Commission** at www.identitytheft.gov
- To the **IRS** at www.irs.gov/uac/Identity-Protection or by calling **1-800-908-4490**. That will prevent tax-fraud thieves from filing tax returns in your name — and collecting your tax refund
- Inform the law enforcement by calling **911** or **GTPD at 404-894-2500**

Tax scams

Report **tax scams**:

- To the **Treasury Inspector General for Tax Administration** at www.treasury.gov/tigta/contact_report_scam.shtml or call **800-366-4484**. Also, report it to the Federal Trade Commission.
- The **Federal Trade Commission** accepts complaints related to many topics (Identity Theft, Telemarketing Scams, Credit Scams...).
    - Read more here: www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc
    - Report a Complaint to the FTC here: www.ftc.gov/complaint

Internet Crimes

Report **internet crimes** (including **SSN theft**, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes):

- To the Federal Bureau of Investigation's **Internet Crime Complaint Center (IC3)** at www.ic3.gov

Immigration Scams

USCIS (U.S. Citizenship and Immigration Services) provides state-by-state information on where and whom to report **immigration scams** and fraud at www.uscis.gov/avoid-scams/report-immigration-scams

Banking Related (leaked bank account information, stolen debit/credit card)

Contact your bank immediately to freeze any and all transactions before attempting to move the money in your account to another account (by using online banking for example).

Georgia Tech Related (phishing attempt sent to Gatech Email, Buzzcards)

- If you receive a message which you suspect may be a **phishing** attack:
  - Forward the message as an attachment to **phishing@gatech.edu**
  - Contact the **Georgia Tech Security Operations Center** immediately at **soc@gatech.edu**
- If your **Buzzcard** has been **stolen/lost**, contact the **Buzzcard Center** (buzzcard.gatech.edu) and **GTPD (404-894-2500)**.

Georgia Tech Office of International Education