Spot the Scams

Fraudulent Text and Email Awareness Resource

As a Sigma leader, you may be a target for online and text scams. Unfortunately, most participants in today's online global community are eventually targeted by a phishing scam or other fraudulent attempt.

Know this: No Sigma Theta Tau International board or staff member will ever ask you to purchase gift cards or wire funds to a third party for any reason.

The best way to protect yourself and your chapter from online and email scams is to educate yourself about how scammers operate and be skeptical of suspicious attempts. Here are some best practices and resources to help you identify a scam and reduce your future vulnerability.

Be aware of the most common scams

Gift card	Someone has an urgent, convincing story asking you to buy a gift card and send them the codes on the back.	Gift cards are the number one scam payment that imposters demand. If you are asked to provide a gift card in response to a text or email, be suspicious.
Lottery / sweepstakes	Must pay a fee to receive your prize	Ignore it; it's not a real prize.
"Guaranteed" loans	Request to pay for your application or taxes before you receive the loan	Destroy the message; do not send the money.
Phishing	Asks for personal details over email (bank accounts, passwords, Social Security number)	Do not reply or click any links! In the US, forward the email to spam@uce.gov.
Charity	Donation requests from a fake charity posing as real one.	Never wire money when donating to charity, regardless of their legitimacy.
Government / foreign dignitary imposter	An unknown person asks you to provide financial information, avoid legal trouble, or help recover a large sum of money and needs your bank account information.	Never provide financial information over email. Email is unsecure.
Fake emergency	Someone pretending to be a loved one claims to be in trouble, and they are asking for you to send cash.	Never send money electronically until you can verify you know the recipient.

List of common scams

Sources: https://consumer.ftc.gov/scams
https://www.finder.com/money-transfer-scams
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud#:~:text=Charity%20fraud%20schemes%20seek%20donations,others%20who%20want%20to%20help.

Remember: Know this: No Sigma Theta Tau International board or staff member will ever ask you to purchase gift cards or wire funds to a third party for any reason.

Sigma chapter leaders and members have been sent fraudulent texts and emails that appear to be sent by Sigma board members. In several cases, chapter leaders received a message appearing to come from the current Sigma President asking the recipient to purchase gift cards or wire money to a fellow member stranded in travel. We have also seen fake emails that appear to originate from a chapter or international board or staff member asking the recipient to pay invoices attached to the email.

How to identify scam messages

- Suspect any request to purchase gift cards as a potential scam.
- Suspect any request for a money wire or Western Union transfer should as a potential scam.
- Suspect any vague invoice or bill you do not recognize as a potential scam.
- Pay special attention to the email address. Often, at first glance, it appears correct.
- Read the entire message, and watch for misspelling and poor grammar that may indicate a scam.
- Check the graphics and branding on the email. Often the branding, if there is any, is a lower quality than you would get from the real, reputable organization.
- Check the contact information and dates. Does the contact information match what you have on file for that individual or organization? Is the date format abnormal?
- Trust your gut. Scams are crafted to create a sense of urgency or panic. If your heart rate rises, be suspicious.

How to avoid being scammed

- Never share private or financial information over email. Email is not 100 percent secure.
- Never reply directly to a suspicious email address or call a number on a suspected scam email. Instead, contact the mentioned organization or individual directly via a trusted, known phone number or email address to verify.
- Never give out your personal information to any stranger through online interaction.
- Never purchase gift cards in response to a text request, and never send gift card information by text or email.
- Never pay an invoice you are not aware of from a vendor you do not recognize. Always call the email sender to verify.
- Vary your passwords. It is recommended that you change your password regularly and avoid common passwords (Never use “password” or “123456,” for example). Make sure your password is as strong as the data you are protecting.

If you are scammed, REPORT IT

- Contact your credit card company, your bank, and the local police. File reports as soon as possible after you discover you were scammed.
- Report fraudulent texts to your mobile phone provider.
- Report phishing emails to your email provider.

Frequently asked questions

1. Why would a scammer target me?

   Scammers are seeking money, and they target anyone and everyone they can. A few staggering statistics about the amount of money acquired through scams can be found on this site: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.

2. How do these scammers get my contact information?

   If *any* information about you is online, it can be data mined. Visit this site for more information: https://en.wikipedia.org/wiki/Data_mining

Helpful links

Identifying scams

- https://staysafeonline.org/blog/5-ways-spot-phishing-emails/
- https://www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/

Email security

- https://www.digitaltrends.com/computing/can-email-ever-be-secure/
- https://eclat.tech/security/what-do-you-mean-my-email-is-not-secure/

Password security

- https://www.menshealth.com.au/most-common-passwords
- https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Reporting scam emails and texts

- Gmail https://support.google.com/mail/answer/8253?hl=en
- USA.gov https://www.usa.gov/stop-scams-frauds
- US Federal Trade Commission https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages