Spot the Scams

Fraudulent Email Awareness Resource

31 January 2019

As a participant in today's online global community, you may be occasionally targeted by a phishing scam or other fraudulent activity. Unfortunately, most people are targeted at some point. You may also be aware that some recent fraudulent emails targeted Sigma chapter leaders.

We want you to be able to protect yourself and your chapter from online and email scams. Here are some general best practices to help you identify a scam and reduce your future vulnerability.

Be aware of the most common scams

Lottery and sweeps	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	Rip it up; 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.
Foreign "dignitary"	An unknown person contacts you to help recover a large sum of money and need your bank account info to help pay fees.	Never provide financial information over email. Email is unsecure.
"Stranded traveler"	Someone pretending to be a loved one claims to be in trouble, and they are asking for you to send cash.	Never send a money transfer until you can verify you know the recipient.

Source: https://www.finder.com/money-transfer-scams

Sigma chapters and members have been targeted by "Stranded traveler" scam listed above. In the most recent case, chapter leaders received a message appearing to come from Sigma President Beth Baldwin Tigges asking the recipient to wire money to a fellow member stranded in travel.

Sigma has also been made aware of 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. Let us be very clear:

No member of the Sigma Theta Tau International Board of Directors or staff will ever request you to wire emergency funds to a third party for any reason.

Protect your money and avoid these scams: Never pay an invoice you are not aware of from a vendor you do not recognize. Always call the email sender to verify.

How to identify scam emails

- Read the entire email message.
    - Pay special attention to the email address. Often, at first glance, it appears correct.
    - Watch for misspelling and poor grammar, as they are indicators of a scam email.
- Suspect any request for a wire or Western Union transfer should as a potential scam.
- Suspect any vague invoice or bill you do not recognize as a potential 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.

Recommended practices to avoid being scammed

- Know that email is not 100 percent secure and is not a place you should share private information.
- 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.
- Vary your passwords.
    - You must 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.

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 here below.

    a. https://www.scamwatch.gov.au/about-scamwatch/scam-statistics
    b. https://www.theguardian.com/money/2018/sep/25/uk-bank-customers-lost-500m-to-scams-in-first-half-of-2018
    c. https://www.consumer.ftc.gov/blog/2018/03/top-frauds-2017
    d. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf

2. How do these scammers get my contact information?

   If *any* information about you is online, it can be data mined. See the following links for more information:
    a. https://en.wikipedia.org/wiki/Data_mining
    b. https://www.moneywise.co.uk/news/2017-10-17/scam-watch-consumers-putting-themselves-risk-giving-away-personal-info

Helpful links

Identifying scams:

- https://staysafeonline.org/blog/5-ways-spot-phishing-emails/
- https://www.thestreet.com/personal-finance/education/phishing-scams-14794737
- https://www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/

Email security:

- https://www.scientificamerican.com/article/its-time-to-admit-that-e-mail-will-never-be-100-percent-secure/
- 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