

Scam Safety

Kaveer Gera's Eagle Scout Project

What are Scams?

What are Scams?

Scams aim to trick you into sending money, revealing personal information, or downloading malware onto your computer.

Primary Scam Types

Primary Scam Types

There are 3 main types of scams: **email**, **web**, and **telephone**.



Scam Warning Signs

Scam Warning Signs

- Spelling or grammar errors are present.
- Incorrect, blurry, or outdated company logos are used.
- There is alarming or urgent messaging, such as a deadline.
- Correspondence uses a generic method of referring to you (“Hi dear,” “Dear valued customer”), instead of your real name.
 - A legitimate company will use your name in its correspondence with you if it knows your name.
- **Web:** The site uses a URL unrelated to the company.
 - Watch out for subdomains; make sure the primary domain is legitimate.
 - URL architecture: `https://subdomain.domain.com`
- **Email:** The email address from a company uses a public domain instead of a company domain.
 - Legitimate companies will use customized domains (customersupport@netflix.com) as opposed to free email providers (netflix@gmail.com).
- **Email:** It claims to be a company or colleague while the email address does not match or is a jumbled mess.

Scam Warning Signs

- Primarily **web** and **email**: urges you to click a link or download something. Companies typically do not ask you to download files via email. You should be able to find it through official mediums, like their website.
- **Telephone**: The caller claims they are from a government organization that you have had no other contact with.
- **Telephone**: An automated sales call from a corporation or someone offering free stuff.
- **Telephone**: The caller is asking for personal information or the voice is automated.

Common Scam Tactics

Common Scam Tactics

- It presents an offer that seems great, but is too good to be true, such as a free gift card or prize.
- The message creates urgency or fear if you do not follow their instructions in order to cloud your judgement.
 - “Your account will be terminated in 24 hours! Click this link!” or “I’m stuck in another country, and I need money fast!”
- Impersonation: the scammer pretends to be a person or company you know.
 - A company has sent you too much money and you must return the balance
 - One of your friends or family is asking for money for transport, for a project, to get out of jail, etc.

Common Scam Tactics

- The scammer uses similar characters in email addresses or URLs (rnark95@gmail.com instead of mark95@gmail.com) to fool you into thinking they're the right person.
- Primarily **web** and **email**: claims your computer has a virus which will delete all your files or reveal your personal information.
- Claims an account has been suspended and prompts you to click a link to reopen your account.
- Buttons often lead to elaborate spoof sites that imitate the legitimate site and steal the account information you enter.

Hello



alhashimyreem7@gmail.com

To



9:37 AM

 If there are problems with how this message is displayed, click here to view it in a web browser.

Google Forms

Hello,

My name is Reem E. Al-Hashimi, I am writing to you to stand as my partner to receive my share of gratification from foreign companies whom I helped during the bidding exercise towards the Dubai World Expo 2020 Committee.

As a woman and serving as a Minister, there is a limit to my personal income and investment level and for this reason, I cannot receive such a huge sum back to my country or my personal account, so an agreement was reached with the foreign companies to direct the gratifications to an open beneficiary account with a financial institution where it will be possible for me to instruct further transfer of the fund to a third party account for investment purpose which is the reason I contacted you to receive the fund as my partner for investment in your country.

The amount is valued at Eu 47,745,533.00 with a financial institution waiting my instruction for further transfer to a destination account as soon as I have your information indicating interest to receive and invest the fund, I will compensate you with 30% of the total amount and you will also get benefit from the investment.

If you can handle the fund in a good investment. reply on this email only: reem.alhashimi@kacao.com

Regards,
Ms. Reem

Formulaire sans titre

REPLIR LE FORMULAIRE

[Créer votre propre formulaire Google](#)

<https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>

From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM



Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit [suntrust.com](https://www.suntrust.com)
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

<https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html>

bit.ly/2gbylhc Tracuda Networks, Inc. All rights reserved. | [Privacy Policy](#) | [Terms of Service](#)



Instagram

FAKE

Hi [REDACTED]

Someone tried to log in to your Instagram account.

If this wasn't you, please use the following code to confirm your identity. Please [sign in](#):

382951

<https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html>

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025



Claim Your Tax Refund Online

We identified an error in the calculation of your tax from the last payment, amounting to \$ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

[Get Started](#)

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

 Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

[UPDATE ACCOUNT NOW](#)

Need help? We're here if you need it. Visit the [Help Centre](#) or [contact us](#) now.

Vn from 557 897 8971



557 897 8971 <ermin.figueroa@masergy.com>
To



Fri 5/22/2020 2:46 PM



This message was sent with High importance.

If there are problems with how this message is displayed, click here to view it in a web browser.

New VoiceMail from +1 (502)-564-6546!

Attention:

A new VoiceMail has been successfully sent to you and is attached to this e-mail.

Below are the details:

VoiceMail from: Accounts Receivable

VoiceMail sender-ID: - VoiceMail705707.waf

VoiceMail Reference: 0089-575-56453

VoiceMail Priority: Very Important

Reception Domain: VoiceMail Service.

[Listen Now](#)

Confidentiality Notice: This VoiceMail originated from verizonwireless.com, may contain information that is proprietary, privileged client communications or work product. If you are not the intended recipient, you are not authorized to read, retain or distribute this email. If you received this email in error, please notify the sender immediately by email and delete all copies of this email.

<https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>

1 Voicemail Recieved

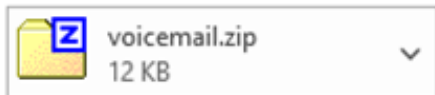


Rahul Sutar <Rahul@pdsol.com>

To



12:28 PM



This letter is from a trusted source

rahul@rackspace.com

You have a voicemail from 1 of your contact

Voicemail will be deleted after 02-12-2021.

This letter with ID: 9e12C8 was sent from a Rackspace Representative .

Rahul Sutar

<https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>

There's issue with your American Express account



American Express <administraciones@pentagon-seguridad.cl>
To



Reply



Reply All



Forward



Fri 11/8/2019 5:29 AM



This message was sent with High importance.

If there are problems with how this message is displayed, click here to view it in a web browser.



Review Your Information.

Due to recent activities on your account, we placed a temporary suspension until you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

[Click here to review your account now](#)

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,

American Express Company. All rights reserved

<https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>

Verifying Legitimacy

Verifying Legitimacy

- **Call the relevant company or person the potential scam is claiming to be.**
 - Ensure you find their contact information *independently* of the information in the suspicious email, website, or phone call.
- **Email:** Check the email address the suspicious message was sent from.
 - If you do not recognize it as who the email sender is claiming to be, it is likely a scam.
- **Web:** Check that the URL primary domain is the company the site claims to be.
- **Telephone:** Ask questions about the organization or ask them to reach out to you in another way.
- **Email** and **web:** Hover over links to see the linked URLs.

Safely Navigating Away from a Scam

Safely Navigating Away from a Scam

- **Web** and **email**: Do not download any files or click any suspicious links.
- **Web**: Close the browser tab or window.
 - If popup windows are preventing you from closing the website, close the entire program.
- **Email**: Delete the email.
- **Telephone**: End the call, don't reveal any personal information, and block the number.
- If you are unsure, seek help from someone you trust (neighbor, grandchild, etc.).

What to Do if You Have Been Scammed

What to Do if You Have Been Scammed

- Remain calm.
- If you shared or entered any passwords or personal information, immediately change the relevant passwords.
- If you sent any money, immediately contact your bank or other issuing financial institution to cancel the money transfer.
- If you downloaded a file, do not open it. Delete it and empty your trash/recycle bin, then run an antivirus scan.
- Don't be ashamed to seek help; scams happen to everyone.

How to Protect Yourself

How to Protect Yourself

- Stay alert for signs of scams; if you are unsure, double-check!
- **Never** send money to anyone you don't know.
- Use reputable antivirus software.
- Routinely change your passwords.
- Always verify information through multiple mediums.

Other Useful Information

Other Useful Information

- If you encounter a scam, report it to the Federal Trade Commission (FTC):
 - reportfraud.ftc.gov (1-877-382-4357)
- **Email:** Report scam emails to the Anti-Phishing Working Group (apwg.org), or forward the email to reportphishing@apwg.org.

Resources

Resources

- scamsafety.kaveergera.com
- Federal Trade Commission (FTC) – www.ftc.gov
- Consumer Financial Protection Bureau (CFPB) – www.consumerfinance.gov/consumer-tools/fraud/
- AARP – www.aarp.org/money/scams-fraud/
- Federal Bureau of Investigation (FBI) – <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes>

Q&A

Thank you

to all of you for coming, and thank you to everyone who helped make this project possible.