

Share

Scam email – common signs

- Unfamiliar or suspicious sender
- Misspellings in domain names
 - such as **rn**icrosoft.com instead of **m**icrosoft.com
- Generic greetings or greeting with your email address
 - ***Hello samspade2643***
- Poor spelling and grammar
- Urgent or threatening language
- Suspicious links or attachments
- Requests for sensitive information
- Odd or irrelevant subject line

Share

Email scams

- frequent topic at Q&A


- Follow-Up - Multiple E-mail Scams (Jan 24, 2024)
 - https://opcug.ca/qa_recordings/20240124_PowerPoint.pdf
- Follow-Up - Another week... another scam (Jan 31, 2024)
 - https://opcug.ca/qa_recordings/20240131_PowerPoint.pdf
- Fraud Watch - Deluge of scam e-Mail (Aug 24, 2024)
 - https://opcug.ca/qa_recordings/20240828_PowerPoint.pdf
- Fraud Watch
 - <https://opcug.ca/fraud-watch/>



Share

Snitcher.space

- Analyzes any email and tells you if it seems likely to be a scam — along with analysis
 - assigns a *Trust Score*
 - tells you how it arrived at its analysis
- Forward email to **scan@snitcher.space**
 - first time, you have to click once on a confirmation email
 - then receive an email back with analysis
- All done through email — nothing to download & install
- Completely free to use
- Snitcher.space says it
 - deletes email after scanning
 - doesn't sell your data
 - <https://snitcher.space/privacy>

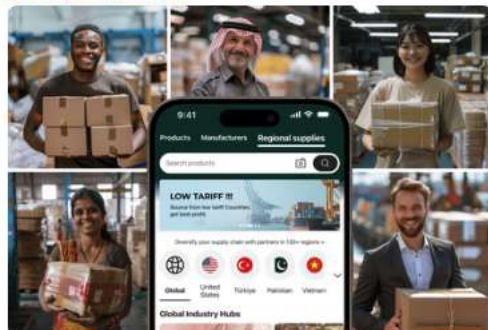
From Sell on Alibaba <global-seller@email.alibaba.com> 

To info@opcug.ca 

2025-07-03, 8:31 p.m.

Subject **More than 100+ buyers want to buy the products you sell, come & see more!**





Say Hello to Your Alibaba.com Store!

Millions of the world's successful brands are sourcing and selling on Alibaba.com. Most of our top sellers begin by creating their own exclusive online stores on Alibaba.com. Whether you're a trading company, wholesaler, or manufacturer, our platform empowers you to reach international markets. As a new seller, you can choose our [Starter Membership](#) for the incredible price of just \$39, which provides a lot of benefits.

Ready to start selling on Alibaba.com?

If you need a personalized consultation, you can email ts_seller@service.alibaba.com.

[Set up Your Store Today](#)

How to Start Selling on Alibaba.com?

See the Procedures Below!



Set up account

Follow a few easy steps to register for an Alibaba.com seller account.



Finish payment

Pay \$39 USD as prompted on the page to enjoy exclusive member benefits.



Complete business verification

"...ing with...
expertise as I keep... market and develop...
Alibaba.com."



Francesco Tamburrino

Rosao Fine Food SRL | General Manager

Showcase Your Brand in Alibaba.com Storefront Today!

Reach global buyers with matching products

[Join Now](#)

[Official Seller Website](#) | [Contact Us](#) | [Business Blog](#)



Read our [Privacy Policy](#) and [Terms of Use](#)

Alibaba.com Singapore E-commerce Private Limited X

Shenton Way, #45-01 AKA Tower, Singapore 068811

Email: DataProtection@service.alibaba.com

[Unsubscribe](#)

[Manage your preferences](#)

Is this a scam?

From snitcher.space <scan@snitcher.space> 📧
To chris.taylor@opcug.ca 📧
Subject [Email Analysis Report] Fwd: More than 100+ buyers want to buy the products you sell, come & see more!

6:10 p.m.

snitcher.space Verified

Email Analysis Report

⚠️ Suspicious Email

Trust Score: 75%

We analyzed an email from **global-seller@email.alibaba.com**.

Here's what we found:

Email Summary

The email is from Alibaba, inviting the recipient to sell on their platform.

Sender Verification

The email originates from global-seller@email.alibaba.com, which appears to be a legitimate Alibaba email address.

Link Analysis

The email contains multiple links to Alibaba.com, which seem to direct to relevant pages for setting up a seller account.

Offer Consideration

The email promotes a 'Starter Membership' for \$39, which could be a legitimate offer but requires caution.

Standard Elements

The email includes standard unsubscribe and privacy policy links, which is typical of legitimate marketing emails.

Summary

This email is an invitation to sell products on Alibaba.com, offering a starter membership for \$39. It includes links to set up a store, contact support, and learn more about selling on the platform.

If you're concerned about potential scams or fraudulent activities while engaging in online business, consider using [Romance AI](#). It's a helpful tool to catch romance scams and other deceptive tactics, ensuring safer interactions.

Report generated based on your request.

© 2025 snitcher.space

[Privacy](#) · [Terms](#)

Trust Score: 75%

- pretty high
- still considered *suspicious*

Legit sender

Legit links

Possibly legit offer of services

Unsub & privacy links

Summary:

- invite — sell on Alibab.com
- links to:
 - set up store
 - contact support
 - learn about selling on Alibaba.com
- I would guess *spam*, not *scam*

From CAA <info@chevitafalit> 
To chris.taylor@opcug.ca  2025-07-15, 12:23 p.m.
Subject **Your FREE CAA Emergency Kit is Waiting - Claim It Today!**



Is this a scam?

DEAR CAA MEMBER,

To thank you for your loyalty, we invite you to participate in a short survey. As a reward, you'll receive **our Premium Emergency Car Kit for free** — no obligations!



Exclusive offer for CAA members

What does your free kit include?

- Premium jumper cables **for emergencies**
- Certified first aid kit
- Accurate tire pressure gauge
- Durable tools **for breakdowns**
- Compact and sturdy bag

Limited availability — Act fast!

GET MY FREE KIT

"This kit saved me twice: once with a dead battery and once with a flat tire."

— John D., CAA member since 2016

Your safety is our priority.

— The CAA Team

[caa.ca](#) [Contact](#) [Privacy](#)

*Offer valid while supplies last. CAA members only.

© 2024 CAA. All rights reserved.

Email Analysis Report

⚠ Suspicious Email

Trust Score: 30%

We analyzed an email from info@chevitafai.it.

Here's what we found:

Summary

The email promises a free emergency car kit to CAA members who complete a survey.

Domain Mismatch

The sender's email address ([@chevitafai.it](mailto:info@chevitafai.it)) does not match the official CAA domain ([caa.ca](mailto:info@caa.ca)), raising suspicion.

Unrealistic Offer

The offer of a free premium emergency kit seems too good to be true, a common tactic in scams.

Generic Greeting

The email uses generic greetings and lacks personalized information, which is typical of mass-distributed phishing attempts.

Suspicious Link

The provided link (flowcode.com) is not directly associated with CAA, adding suspicion.

Summary

This email claims to offer a free emergency car kit to CAA members in exchange for completing a survey. However, the sender's email domain is not associated with CAA, and the offer seems too good to be true. The link provided also raises suspicion.

Trust Score: 30%

Domain mismatch

- [@chevitafai.it](mailto:info@chevitafai.it) doesn't match official domain [@caa.ca](mailto:info@caa.ca)

Unrealistic offer

Suspicious link

- [Flowcode.com](https://flowcode.com) not associated with CAA



Summary:


- offer free emergency car kit
 - for filling out a survey
- Problems with
 - email domain
 - seems too good to be true
 - suspicious link
- I would guess **scam**

From iCloud Inc. <0e15y376@xn--2i0bt1gxrhga544iwp.com> @

To chris.taylor@opcug.ca @

2025-07-19, 8:07 a.m.

Subject **URGENT: Update Your Payment Information to Avoid iCloud Service Disruption**

 To protect your privacy, Thunderbird has blocked remote content in this message.



Options ▾

Apple Logo

Urgent: Update Your Payment Information

Dear Valued Apple Customer,

We have encountered an issue while processing your recent payment. To avoid any disruption to your services, we kindly request that you update your payment details immediately.

Failure to update your payment information may result in the following consequences:

- **App Store Purchases:** Your apps, games, and purchases will be canceled.
- **iCloud Storage:** Your data backups may be permanently lost.

Please click the button below to securely update your payment details:

[Update Payment Information](#)

You have 72 hours from the time of this notice to update your payment information. Failure to do so will result in service interruption. Thank you for your immediate attention to this matter.

Best regards,
The Apple Team

This message is intended for Apple customers only. If you received this email in error, please disregard it.

Perhaps the most obvious scam

- even if **you** would **never** fall for it, maybe some would!
- or **you might**, when
 - in a hurry
 - tired
 - not paying attention
 - ...

Email Analysis Report

Scam Email

Trust Score: 10%

We analyzed an email from **iCloud Inc.**
<0e15y376@xn--2i0bt1gxrhga544iwpix.com>.

Here's what we found:

Urgency and Pressure

The email uses urgent language to pressure the recipient into updating their payment information.

Suspicious Sender Address

The sender's email address (0e15y376@xn--2i0bt1gxrhga544iwpix.com) is suspicious and does not match Apple's official domain.

Suspicious Link

The link provided for updating payment information (email.mg2.substack.com) is not an official Apple domain.

Threats and Consequences

The email threatens service disruption and data loss if payment information is not updated within 72 hours.

Summary

This email claims to be from Apple, stating that there was an issue processing a recent payment and urges the recipient to update their payment information to avoid service disruption and data loss. The email contains several red flags, including a suspicious sender address and a non-Apple link.

Trust Score: **10%**
• Classified as **Scam**

Urgency & pressure

Suspicious sender
• doesn't match Apple domain

Suspicious link
• link to update payment info not Apple domain

Threats & consequences

Summary:
• claims to be from Apple
• several red flags including
• suspicious sender address
• non-Apple link

Share



snitcher.space

Verified

- Gives hints and clues about elements frequently manipulated by scammers
- Exposes some hidden elements
 - e.g. where an *Update payment* link actually goes
- Aggressive in labelling *some* legit emails as *Suspicious*
 - free 3-month trial for Microsoft 365 Personal after buying a computer from Costco
 - email from Google about new Gemini features
- Service is sometimes quite slow
- See <https://snitcher.space/> for details:
 - how it works
 - scams they detect
 - scam detection technology
 - FAQs

Another tool in your toolkit