

Phishing Information

- [Example Phishing Message](#)
- [Reading Email URLs](#)

Example Phishing Message

Below is an example phishing message.

Email Preview - Timesheet Correction×

From: Amy Chan <achan@gorgeandbell.com>
Reply-To: Amy Chan <achan@gorgeandbell.com>
Subject: Timesheet Correction - April 2023
📎 april_2023_timesheet.xlsx

Template ID: 484507-00d575f1-6ceb-4a7a-a46a-5f37ac64fe3a
[Send Me a Test Email](#)

Hi Tyler,

I'm just going through this months timesheet entries and noticed a mistake with yours. Could you please review the attached section and let me know if its correct?

Thanks,

Amy Chan
Office Manager

Direct: 604-259-6694 Toll free: 888-800-1450
achan@georgeandbell.com
M2-601 West Broadway, Vancouver, BC V5Z 4C2
I acknowledge that my place of work is located on the traditional, ancestral and unceded territories of the xʷməθkwəy̓əm (Musqueam), Skwxwú7mesh (Squamish), and Səlilwətaʔ/Selilwitulh (Tsleil-Waututh) peoples.

Close

On first glance, the message looks completely legitimate. The email signature is correct, the email looks correct, the message is something that you would expect to receive and the attachment seems benign. There is really only one large give away and that was the sender email address. In it you can see that the “gorgeandbell.com” is missing the “e”. Another more subtle hint that may not give it away but is a potential red flag is the vagueness of the message. “Amy’s” request has no specific information regarding the request, other than to look at the attachment.

Here are some quick tips to avoid falling into the trap and opening a phishing such as the one above:

1. Always hover over and check the underlying link before clicking. Ensure the domain matches the message. For example a message from Microsoft should have a URL that ends in .microsoft.com.
2. Check and verify the sender address. Make sure it doesn't have any spelling mistakes.
3. Don't open any attachments unless you've confirmed that the message is legitimate.

4. Keep a close eye on content of the message. Does the message sit right with you?
5. If you're ever unsure, call the individual and have them verify the message.

Reading Email URLs

All email messages have their URLs modified so when clicked you're directed to our spam filtering provider prior to being redirected to the original URL. This allows our spam filtering provider to scan and verify the legitimacy of the link before redirecting you to the site. If the site is found to be malicious, your attempt to access the site is blocked.

The downside of this service is that it makes verifying a link a little bit more difficult due to the added text the service adds to the URL. Below is information on how to read through this added information so you can manually check and verify the URL before proceeding.

Below is an example of what a link will look like within an email message.

To see this URL within an Office application, hover over a link for a few seconds.

`https://url.avanan.click/v2/___https://google.com/___bXQtCHjvZC1hdi1jYS0yOmNh (shortened)`

To read through this text and validate the original URL, look for the underscores within the link. The address between the underscores is always the original website. In this case, the original URL is:

`https://google.com/`

If the address looks legitimate and safe, you know it's safe to click and view.