IT Support

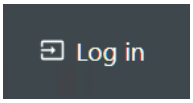
Connecting with IT for assistance.

Accessing IT Documentation

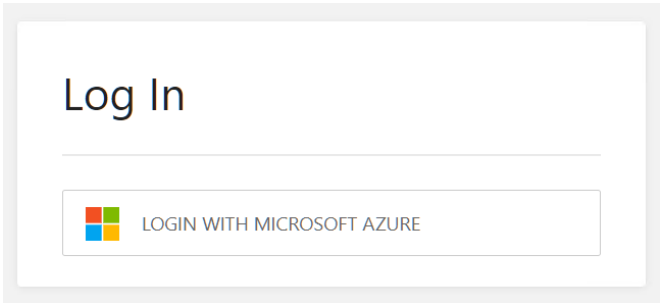
This article will walk you through the registration process to access George & Bell's IT documentation. To complete this process, you'll need to have your Microsoft 365 credentials ready and available.

Instructions

1. Select **Log in** from the top right-hand corner.

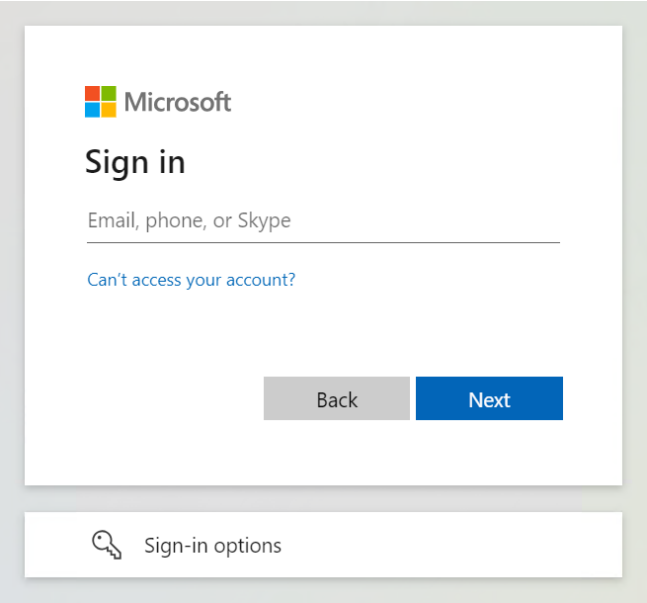


2. Select **Login with Microsoft Azure**. You'll be taken to Microsoft 365 and asked to sign-in.

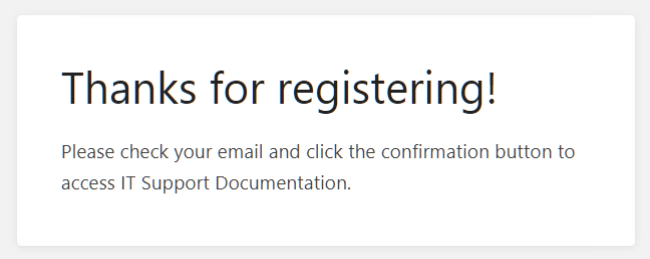


3. Logon using your Microsoft 365 credentials.

> If signing in via a work laptop, Single Sign-On (SSO) will automatically sign you in.



4. Once successfully signed into Microsoft 365, you'll be sent an email asking to validate your email address. Open the email and click on the provided link to confirm your email address.



5. You have successfully registered. Select **Shelves** in the top bar to see all available articles.

Reporting an IT Security Incident

In the event that you suspect that your laptop or account has been compromised, whether via a malicious actor, virus or malware. Please do as follows.

1. Do not shutdown your laptop.

Depending on the type of attack, shutting down your laptop can cause useful information to be lost if its a larger breach by a malicious actor. It's best that the laptop be left untouched so a security professional can investigate prior to taking action.

2. Call IT Support.

Please immediately call IT Support to report the issue so it can be investigated and escalated if necessary.

What happens afterwards?

If the incident is isolated to your laptop but further investigative work is required, you'll be provided with a spare to allow you to continue working in the meantime. For larger incidents you'll receive further instructions from IT Support or directly from the partners.

What Constitutes a IT Security Incident?

An IT Security Incident is any technology based attack which may compromise the confidentially of our company or that of our clients. An IT Security Incident can include:

- Virus/malware infections.
- Keyloggers (records what you type on your keyboard).
- Data exfiltration whether via an external entity or an employee/contractor.
- Data breaches.
- Ransomware attacks (encrypts all data requiring payment to decrypt).

Communications

Requesting Support

If you have a question or issues related to IT, please reach out to the IT department. The IT department can be reached Monday thru Friday, 9:00am to 5:00pm through the following channels:

Email: itsupport@georgeandbell.com
Phone: +1 (604) 259-6583

When reaching out to IT support, please be prepared to provide the following information:

- A phone number technicians can best reach you at.
- A detailed description of the issue you are experiencing.
- Screenshots of any of the error messages you may be receiving.

If internal IT is not available due to being on vacation etc. ITS Consulting is available to assist. They can be reached through the following channels:

Email: help@itsmail.ca
Phone: +1 (604) 484-4300

Emergency After-Hours Support

If you have an issue that affects the entire company and would like to report it, please call 1-604-259-6583. If internal IT is on vacation, please call ITS Consulting at 1-604-484-3400. Do not select any option when calling in. Alternatively email help@itsmail.ca.

Safe Communication Channels

This article has been written to provide confidence that you communicating with an authorized individual. If you have any doubts regarding an received email or phone call please follow the directions outlined under *Phishing Attempt Response* (below).

Technical Communications

Technical support is primarily handled in-house by Tyler Rasmussen, however a backup Managed Service Provider (MSP) has been contracted to provide IT support in case of Tyler's absence. Please vet all calls and emails purporting to be from IT to ensure their legitimate.

Phone calls should always originate from one of the following numbers:

- +1 (604) 259-6583 (Internal IT Support)
- +1 (604) 484-4300 (ITS Consulting)

All support based email communications will always originate from one of the following email address:

- itsupport@georgeandbell.com
- trasmussen@georgeandbell.com
- dispatch@itsmail.ca

> Staff wide IT announcements, infrastructure changes, scheduled maintenance and requests for information will always come directly from Tyler Rasmussen:
>
> trasmussen@georgeandbell.com.

> Please note, admin@georgeandbell.com and tyler.rasmussen_a@georgeandbell.com are valid internal email addresses however you should never receive any communications from these email accounts.

Partner & Managers

Partners and managers at George & Bell will only communicate company information **via their own work email address**. If you receive an email from a partner or manager that was not sent directly from their work account, please forward the message to IT for investigation.

The partner email addresses are:

Brendan George	bgeorge@georgeandbell.com
David Lee	dlee@siss.ca
Greg Heise	gheise@georgeandbell.com
Jeremy Bell	jbell@georgeandbell.com
Mackenzie Bell	mbell@georgeandbell.com
Mike Greschner	mgreschner@georgeandbell.com

Administration

You may receive email communications from the Administration department. Administration staff include:

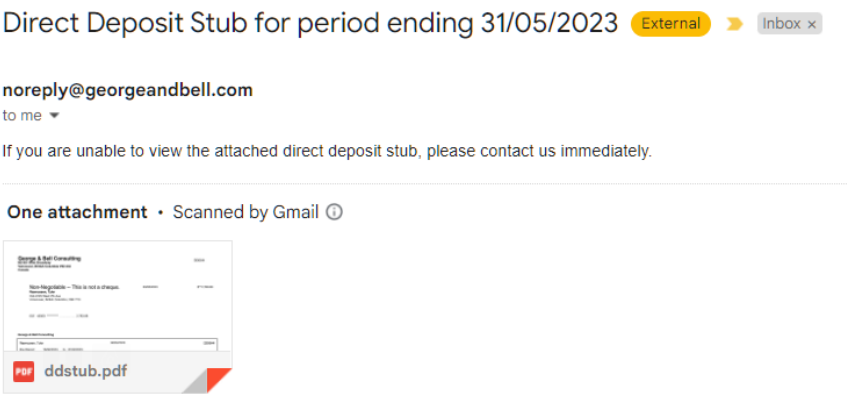
Amy Chan	achan@georgeandbell.com
Mackenzie Bell	mbell@georgeandbell.com

Additionally, the administration staff use the following mailboxes for specific purposes:

Info (public inquiries)	info@georgeandbell.com
Accounts Payable (for receiving invoices and receipts)	accountspayable@georgeandbell.com

Paystubs

Paystubs are sent from the email account noreply@georgeandbell.com and will look as follows:



Services

Scanned Documents

Documents scanned by Printer F within the copier room will be send via the noreply@georgeandbell.com email account. If you were not expecting a scanned document, do not open the attachment until confirmed that it's legitimate.

KnowBe4

Messages from KnowBe4 will arrive from do-not-reply@knowbe4.com. Messages will typically consist of notification regarding enrollment or that a training campaign needs to be completed.

1Password

Messages from 1Password will arrive from no-reply@1password.com. Messages will typically consist of invites onto its services or notification around managing your account.

Duo Mobile

Message from Duo Mobile will arrive from no-reply@duosecurity.com. Duo will rarely send out email messages. The only message to expect from Duo is the initial enrollment email.

Microsoft 365

Microsoft sends notifications from a variety of different email accounts, however consistently all accounts end in @microsoft.com. Please know Microsoft will **never** send you message asking you to:

- Check a voicemail message.
- Change a password.

LiquidFiles

Message from LiquidFiles will arrive from noreply@georgeandbell.com. LiquidFiles will only send messages relating to sending and/or receiving files.

Phishing Attempt Response

If you receive an email or call from someone purporting to an IT technician and their phone number or email is not on this list please:

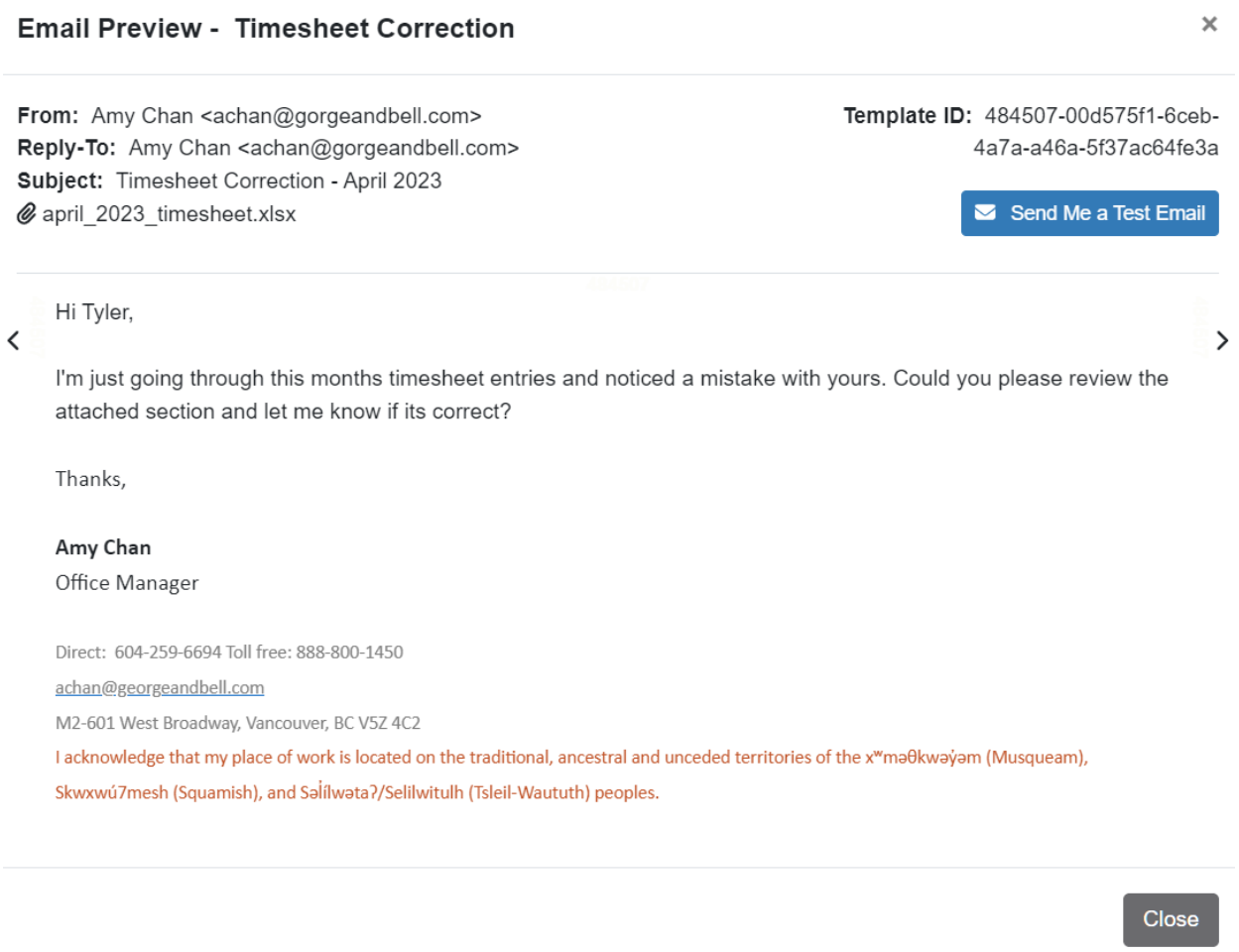
1. Hang up and refuse to speak with the caller. If via email, do not reply or open any links or attachments.
2. Notify your manager CC'ing Tom and Brendan.
3. Retain any information you may have on the call/email for future investigation.

Phishing Information

Phishing Information

Example Phishing Message

Below is an example phishing message.



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 your directed to our spam filtering provider prior to being redirecting to the original URL. This allows our spam filtering provider to scan and verify the legitimately 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 its safe to click and view.

Vancouver Office Seating Map

The following diagram outlines what number each desk within the office is labelled as. For example, the desk nearest the kitchen would be considered K1.