519-741-2312 building@kitchener.ca www.kitchener.ca/building

Phishing Email Warning & Cyber Security Tips for Customers

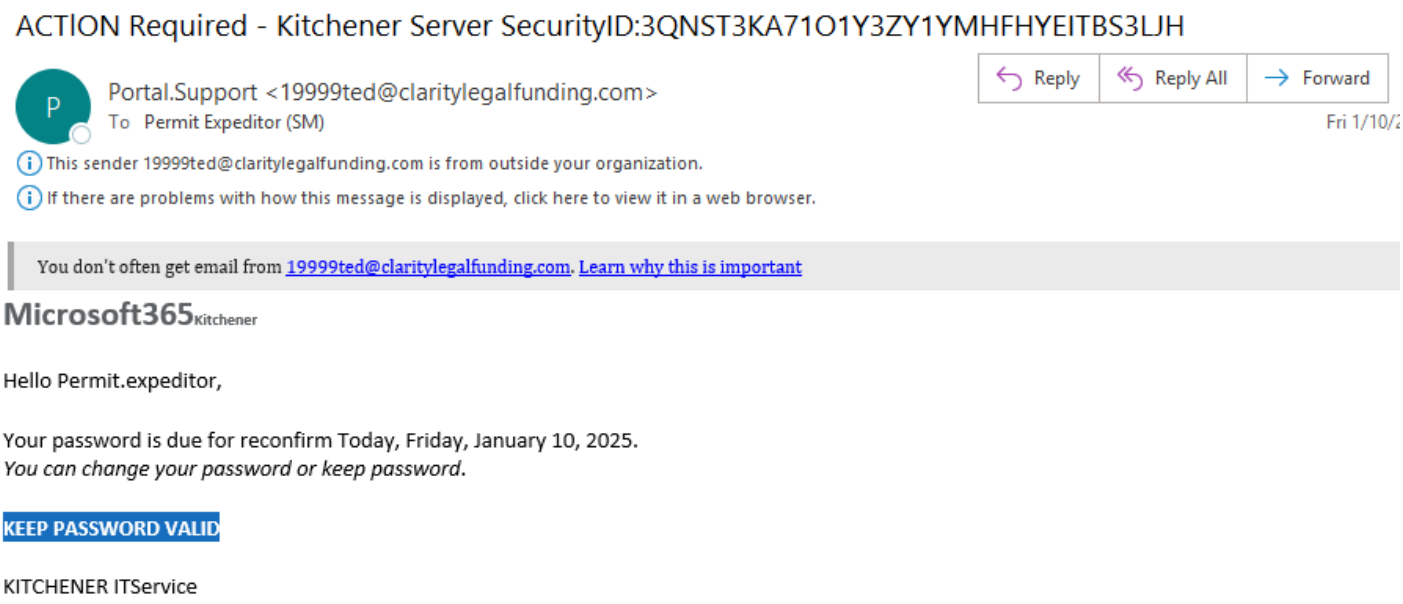
Jan. 13, 2025
BB 2025-01

In today's digital world, it's essential to stay vigilant against potential cybersecurity threats.

Recently, we've learned that some customers have received phishing emails falsely requesting a reset of their City of Kitchener permit portal passwords. These emails are **not legitimate** and do not originate from an @kitchener.ca email address.

To assist with your awareness, we've included an example of the phishing email below;

Example:


ACTION Required - Kitchener Server SecurityID:3QNST3KA71O1Y3ZY1YMHFHYEITBS3LJH

Reply | Reply All | Forward

P Portal.Support <19999ted@claritylegalfunding.com>
To Permit Expeditor (SM)
Fri 1/10/2

This sender 19999ted@claritylegalfunding.com is from outside your organization.
If there are problems with how this message is displayed, click here to view it in a web browser.

You don't often get email from 19999ted@claritylegalfunding.com. Learn why this is important

Microsoft365 Kitchener

Hello Permit.expeditor,

Your password is due for reconfirm Today, Friday, January 10, 2025.
You can change your password or keep password.

KEEP PASSWORD VALID

KITCHENER ITService

We're also sharing some key tips on the next page to help you recognize and avoid phishing attempts so you can stay informed and protected.

Cyber Security Tips

Below are some practical tips to help you identify suspicious emails and protect your personal information:

1. **Verify the Sender's Email Address**
   - Look closely at the sender's email address.
   - Ask yourself: Is it coming from a legitimate **@kitchener.ca** address?
   - Watch out for slight misspellings or odd domains that try to mimic legitimate sources.

2. **Examine the Links Before Clicking**
   - Hover over any links in the email (without clicking) to see the actual destination URL.
   - Does the link match what you expect? For example, if it appears to point to YouTube, consider whether a link to YouTube makes sense in the context of an email from the Building Division.
   - Be cautious if the URL looks strange, misspelled, or unrelated to the message.

3. **Consider the Reasonableness of the Email**
   - Think critically: Is it reasonable that the Building Division would send you this email?
   - Does the tone, content, or subject align with the type of communication you normally receive?
   - If the email seems out of character or unexpected, it may be a phishing attempt.

4. **When in Doubt, Verify with Us**
   - If you're unsure whether an email is legitimate, do not click on any links or download attachments.
   - Contact us directly using a known and trusted communication method (e.g., phone number or email address you've used before).
   - We can confirm whether the email is legitimate and provide guidance if it's not.

Additional Tips

- **Avoid Sharing Personal Information**: Never provide sensitive information like passwords or account details via email.
- **Be Wary of Urgency**: Phishing emails often create a sense of urgency to trick you into acting quickly. Take your time to verify.
- **Keep Software Updated**: Ensure your devices, browsers, and antivirus software are up to date to protect against the latest threats.

By following these tips, you can stay one step ahead of cybercriminals and ensure your information remains secure. If you ever have questions or concerns, we're here to help!