21st Century
TRAVEL INSURANCE LIMITED

DON'T GET TRICKED

Avoid Phishing Emails

Image designed by Freepik

THE MOST BELIEVABLE PHISHING PAGES TRICKED USERS 45% OF THE TIME!

Source: Google, Behind Enemy Lines in our war against account hijackers (Nov. 2014)

WHAT IS "PHISHING"?

Phishing emails are designed to appear as though they come from a trusted individual or organization. However, they are actually sent by cybercriminals attempting to deceive recipients into clicking on malicious links or opening harmful attachments, which can compromise their computer and sensitive information.

WHY ARE YOU AT RISK?

Cybercriminals actively target both businesses and individuals to access valuable information. They are particularly interested in financial, customer and employee data, including credit card numbers and passwords. In a business setting, a single successful phishing attack can compromise the entire organization, leading to significant security and financial risks.

HOW TO MANAGE RECEIVING A SUSPCIOUS EMAIL

If you suspect that an email is a phishing email:

- Avoid clicking on any links or opening attachments.
- Do not reply to the email.
- Permanently delete the message.
- Report the email using your provider's spam or phishing tools, or notify your IT department if applicable.

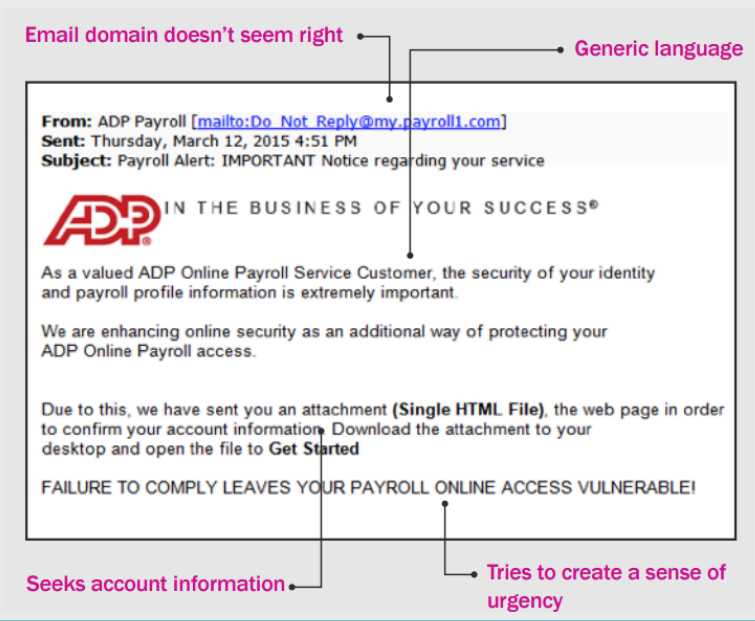
WHAT TO DO IF YOU ALREADY OPENED A LINK OR ATTACHMENT

- Write down as many details of the attack as you can recall. Try to note any information such as usernames, account numbers or passwords that you may have shared.
- Immediately change the passwords on all affected accounts and anywhere else that you use the same password.
- Confirm that you have multi-factor (two-step verification) turned on for every account you can.
- If this attack affects work accounts, disconnect your device from the internet and notify your IT department.
- Notify any impacted clients.
- Don't hesitate to report it to law enforcement if there is a financial loss or identity theft.

HOW TO SPOT A PHISHING EMAIL

Hackers are getting clever in how they design emails they send out to make them look legitimate. Phishing emails often have the following characteristics to help you spot them:

1. They ask for your username and/or password.
2. They have grammatical and spelling errors.
3. They have generic greetings.
4. They contain email addresses that don't match between the header and the body, are misspelled or have unusual formats.
5. They have links or email addresses that show a different destination if you hover over them.
6. They try to create a sense of urgency about responding or are threatening.
7. They have suspicious links or attachments.



21st Century Travel Insurance
18-1040 Division St. Cobourg, ON K9A 5Y5
1-800-567-0021
info@21stcenturytravelins.com