

How to Identify an Email Phish

Do not respond to links that ask you to enter your username or password.

1. Email is sent from someone impersonating a Prairie Spirit employee

It is possible to impersonate someone using their email address. If you receive instructions from your supervisor or a colleague that seem unusual, double-check their validity using an alternate means of communication.

2. Unexpected attachments

An email contains an attachment when you were not expecting one or you do not recognize the sender or the sender's email domain.

3. Creating a sense of urgency or threatening tone.

The email is pressuring you to take action right away or else there will be a negative consequence. Such examples are pending account closures, CRA tax errors or verifying a purchase.

4. Payment demands from reputable sources

An email appears to come from a reputable source demanding payment right away using unconventional means such as BitCoin (or other crypto currencies), gift cards or pre-paid credit cards.

5. Poor grammar and spelling

An email contains very poor grammar such as "If you take no action you account will be suspended."

6. Email greeting is generic and/or non-specific

Emails that use generic greetings will sometimes begin with "Dear user" or "Dear firstname.lastname". Someone sending a legitimate email will know who you are.

7. Don't trust names and logos alone

Real names, logos and other information can be placed in emails to create more convincing impersonations of individuals or groups that you trust. If an email contains a logo, it doesn't mean that the email is legitimate.

8. Email looks legitimate but still are not sure, verify by another means

When in doubt on the legitimacy of an email, it is recommended to contact the alleged sender through a separate means (ex: by phone) to confirm the email. If you think you need to confirm something that is being said in the email, go directly to your account page instead of opening a suspicious looking link that claims to take you to your login page.

If you are ever in doubt or think you may have clicked a link or opened a bad attachment, contact the Help Desk. We can help re-secure your account to limit abuse and data loss by bad actors.

Web
helpdesk.spiritsd.ca

Email
help@spiritsd.ca

Phone
306-683-2931