Dear

Following on from Victoria's email earlier today concerning a data breach, we are writing to inform you that some of your personal data may have been visible to an external person. This is in association with a recent security incident involving one of our VET.CT Gmail accounts. We understand the importance of protecting your personal information and we want to be transparent about what happened and the steps we've taken.

This document outlines what happened and the steps that we have taken so far (see below).

The security breach occurred in relation to a member of our finance team. The finance team handles sensitive information within their email correspondence as part of their daily role here at VET.CT. We believe that if the external person had so wished, then they would have been able to see this information contained within an email sent by this member of the finance team to our payroll provider or to you directly. This included the following personal details for you:

- Your Social Security Number and home address that was emailed to you in your 1099

It is important to note that the risk of your data having been accessed is minimal. We have identified that no downloads of data occurred from the account. Therefore, for your data to be accessed it would have required the individual hacker to open one of over 10,000 emails and screen-shot the details from a single email.

In terms of next steps you should take, please look out for any suspicious activity related to your personal information. If you have any concerns that your personal data may have been used or compromised then please contact the IT team by submitting a ticket here. Please also read and follow the advice of the relevant reporting authority for your region which is linked here and contact your bank and follow their advice.

If you have any other questions or concerns please contact me directly.

Kind regards

Mandy

Hi everyone,

I am writing to let you know about a data breach incident that has occurred and that we have been made aware of. We deeply respect the privacy of data here at VET.CT and this email is aimed at giving you as much information as possible so that you can understand what has happened and what steps we are taking.

How did the data breach occur?

An external person gained access to a single VET.CT Gmail account on 23rd March 2025 and we believe that this was almost certainly as a result of a successful phishing attempt. Phishing is where an attacker uses an email, text message or other scam to fraudulently gain access to an account. Nothing suspicious occurred until 7th April 2025 and on that date the external person sent an internal email requesting that a payment should be set up. At this time, a member of our team became suspicious and notified VET.CT that an email account had been compromised and no such payment was made. Our IT team then took immediate action to secure the affected account, and a full investigation into the extent, impact and management commenced.

Investigation

A comprehensive internal investigation has taken place over the last 48 hours. This has enabled us to understand the extent of the breach. This involved a detailed analysis of the Gmail account in question as well as a review of other email addresses and company systems to ensure that the breach is limited only to this single user.

Results of investigation

The investigation has confirmed that the breach was limited to a single user and Gmail only. The user is a member of our support team and as part of their daily job had sent/ received emails with some personal information within them (e.g. home address). We have a list of these individuals and the personal information that could have been visible to a hacker, and we will be notifying you separately today. If you do not receive any further communication from us then you can be assured that we have not identified any of your personal information within the user's emails.

Actions taken

As well as securing the user account in question, all other accounts and software access for the user have had their passwords changed. We are reporting the breach to the relevant authorities in line with required protocol. There will be a full review into how this breach

occurred and what we can learn from it in terms of what additional measures we can take to reduce the risk of future events.

What is the risk to my personal data?

If you are one of the people whose personal information was contained within the user's email account then it is important to note that the risk of your data having been accessed is minimal. We have identified that no mass downloads of data occurred from the account. Therefore, for your data to be accessed it would have required the individual hacker to open one of over 10,000 emails and screen-shot the details from a single email.

If the risk is so low, why are you telling me about it?

We deeply respect the privacy of your personal information and are informing you as a precaution. We are sending this email to all team members to encourage you to be extra vigilant and understand exactly what has occurred. For those who may have been affected, we will email you individually with more details. We understand this may cause concern and inconvenience and we want to answer your questions and support you in any way we can.

What should I do now?

Please be vigilant and if you notice any suspicious activity related to your personal information, then please contact the IT team by submitting a ticket here. Please also read and follow the advice of the relevant reporting authority for your region (linked at the bottom of this email) and follow the advice.

Could VET.CT have prevented this situation?

Regrettably, hacker activity and cyber attacks are impossible to prevent entirely. While VET.CT has appropriate measures in place to mitigate risk, those engaged in online crime are constantly working to circumvent protection measures. We regularly review our protections to ensure they are up to date, and will conduct an additional review following this incident. However, even with the most robust measures in place, data cannot be completely secure.

What can I do to help?

If you have not done so already, please set up two-factor authentication (2FA) on your Google account as a priority - follow the guidance linked here.

VET.CT regularly offers cybersecurity training to all of our employees and contractors. It is incredibly important to complete these training opportunities when they are offered. This

helps all of us remain aware and vigilant regarding all forms of cyber attacks within VET.CT and beyond.

I have more questions who should I contact?

Please contact people@vet-ct.com if you have any more questions or would like to speak with us.

Thank you for reading this email and for your understanding,

Victoria

Find out more about how you can protect your personal information through the following links:

Australia: https://www.servicesaustralia.gov.au/protecting-your-personal-information-after-data-breach?context=60271

Canada: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/

UK: https://www.ncsc.gov.uk/guidance/data-breaches

USA: https://www.usa.gov/identity-theft