



# Phishing – awareness and training



# Phishing email

Your February bill for Account 42 [redacted]

2013-1-1.jpg 18 KB

From: Vodafone <[YourVodafone@financialadvicers.com](mailto:YourVodafone@financialadvicers.com)>

Sent: [redacted]

To: [redacted]

Subject: Your February bill for Account 42! [redacted]

**JPG made to look like a PDF**

**Not from a Vodafone email address**

**Links do not go to Vodafone website**

**Misspelt words**

**Sense of urgency**

20 February 2021

**My Vodafone bill**  
[Vodafone.co.nz](http://Vodafone.co.nz)

Hi there,  
Please find your Vodafone bill attached. If you need help with understanding your bill, please visit [Vodafone.co.nz/billing](http://Vodafone.co.nz/billing)

**How to pay your bill**

Original URL:  
<https://financialadvicers.com/route.php?token=7209e5b1d2a0be8962c13f7bf0b2cddb0825d3ea>  
Click or tap to follow link.

Stripe payment processing platform. You will need to update your payment

[Update your details now](#)

**Recieve a 10% discount on your bill when you update your details and pay by 24th February 2021**

My bill  
Due on 13 Mar 21



# Genuine email

Your February bill for Account 42! [redacted]

60485-221 KB pdf

From: Vodafone <[YourVodafone@bills.vodafone.co.nz](mailto:YourVodafone@bills.vodafone.co.nz)>

Sent: [redacted]

To: [redacted]

Subject: Your February bill for Account 42! [redacted]

**PDF attached**

**From a Vodafone email address**

**Links go to Vodafone website**

20 February 21

**My Vodafone bill**  
[Vodafone.co.nz](http://Vodafone.co.nz)

My bill  
Total: 6 [redacted] incl. GST  
Due on 13 Mar 21

Hi there,  
Please find your Vodafone bill attached. If you need help with understanding your bill, please visit [Vodafone.co.nz/billing](http://Vodafone.co.nz/billing)

**How to pay your bill**

Direct debit from your bank account or your credit or Visa debit card is a simple, safe and convenient way to pay your bill. Once it's set up, your monthly bill will be paid automatically on the due date.

Original URL:  
[https://help.vodafone.co.nz/app/pci/direct\\_debit/%20/425438691/](https://help.vodafone.co.nz/app/pci/direct_debit/%20/425438691/)  
Click or tap to follow link.

[Set up a direct debit now](#)

If more than one signature is required, complete and sign the [Bank account direct debit form](#) and post to the address provided or scan and email to [nzcustomerpayments@vodafone.com](mailto:nzcustomerpayments@vodafone.com)

Phishing scams mimic legitimate emails –  
Observe carefully!

# Check the sender's email address




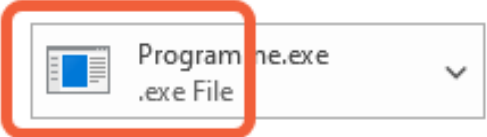
## Who sent the email?

<p>Vodafone &lt;YourVodafone@financialadvisers.com&gt;</p> <p>← That's not Vodafone!</p>	<p>Check the email domain matches the sender's address</p>
<p>Norton Antivirus &lt;Norton@employee-portal.com&gt;</p> <p>← That's not Norton!</p>	
<p><u><a href="mailto:John.Doe@midcentraldhb.govt.nz">John.Doe@midcentraldhb.govt.nz</a></u></p> <p><u><a href="mailto:John.Doe@midcentrαldhb.govt.nz">John.Doe@midcentrαldhb.govt.nz</a></u></p>	<p>Can you spot the difference?</p> <p>Check addresses carefully, hackers are super sneaky</p>

# Check the attachments



## Risky attachments or actions

	<p>This attachment is a picture of the PDF logo. The genuine email has a PDF attachment, so the phishing email needed to look the same.</p>
	<p>Programme files like .exe and files with macros like .docm can contain malware. <b>Do not click</b></p>
<p>Please use the form below to change your password.</p> <ul style="list-style-type: none"><li>* Current Password: <input type="password"/></li><li>* New Password: <input type="password"/> Weak</li><li>* Confirm Password: <input type="password"/></li></ul> <p><input type="button" value="Reset Password"/></p>	<p>If you are asked to sign in – <b>abort!</b> You may be giving away your username and password.</p>

# Check the links' addresses



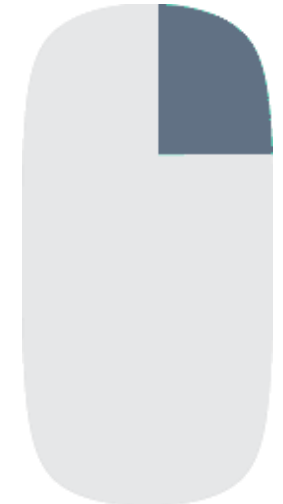
## Dodgy links

Vodafone  
As part of details.  
[Update your details now](#)

Original URL:  
<http://financialadvisers.com/ro...>  
token=cd2886c1e3b5ca48d55872432f0  
03cca2ada783c  
Click or tap to follow link.

That's not  
Vodafone!

Right click on or hover over a link to see the linked website address



mail on [redacted] has  
n ma <https://employee-portal.com/ro...>  
k=1022a63564ec390f95be8b9c0eb772  
26d1718bfa  
rou s  
Click or tap to follow link.  
[CONTINUE WITH SCANNING](#)

The email  
claimed to be  
from Norton

# Beware a sense of urgency



## What's the hurry?

**Recieve a 10% discount on your bill when you update your details and pay by 24th February 2021**

**Urgent notification! Malware Attack**

Status: Compromised

*If not corrected immediately your account will be exposed to hackers.*

Password expiry notice!

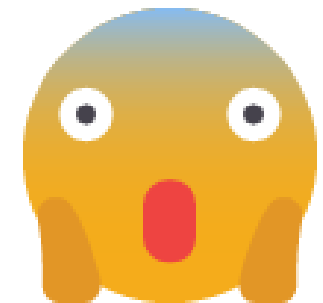
You need to retain or change your password now to avoid login issues related to your account.

Follow the button or link below to retain current password.

Due Date: **Wednesday, June 23, 2021 10:04am**

<https://outlook.office.com/mail/resolve>

Hackers pressure you to act quickly so you don't have time to think about what you're doing



# Notice impersonal or incorrect greetings



## Do you know me?

<p>Dear You</p> <p>URGENT Updates - READ NOW</p>	<p>Phishing emails are often addressed impersonally</p>
<p>Dear valued customer,</p> <p>You are require to update</p>	
<p>Confirm Your Identity:</p> <p>with your User ID: <a href="#">Sign in to the customer portal</a></p> <p>Name: Ke [redacted] ell</p> <p>User ID: <a href="#">ke [redacted] nz</a></p>	<p><b>But not always</b> - hackers can find your name and email online and use them in phishing emails</p>

# Notice poor grammar and/or spelling



## That's not quite right

Recieve a 10% discou  
your details and pay |

You are require to update your  
prevent account termination. F

This invoice is sent repeatedly,  
possible time

It can be easy to miss grammar and spelling mistakes when reading quickly

**Take the time to notice these**





# Can you spot a phishing email?

Click the fish to take a test



# What to do when you've been phished?



If you see something – say something

**Inform your IT provider IMMEDIATELY** - They will know what to do depending on the nature of the phishing attack



