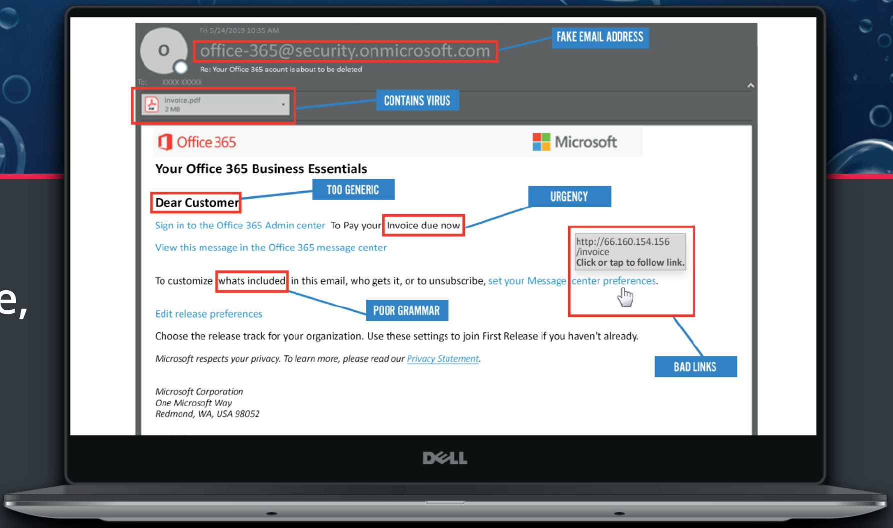
access
freedom to do more

ID AGENT PARTNER

# Tips for detecting a phishing email

Cyber criminals might send an email that looks legitimate, known as a phishing email, but you can take steps to avoid the traps



Fri 5/24/2019 10:35 AM

office-365@security.onmicrosoft.com

Re: Your Office 365 acount is about to be deleted

To: XXXX XXXXX

invoice.pdf
2 MB

Office 365 Microsoft

**Your Office 365 Business Essentials**

Dear Customer

Sign in to the Office 365 Admin center To Pay your Invoice due now

View this message in the Office 365 message center

http://66.160.154.156/invoice
Click or tap to follow link.

To customize whats included in this email, who gets it, or to unsubscribe, set your Message center preferences.

Edit release preferences

Choose the release track for your organization. Use these settings to join First Release if you haven't already.

*Microsoft respects your privacy. To learn more, please read our Privacy Statement.*

*Microsoft Corporation*
*One Microsoft Way*
*Redmond, WA, USA 98052*

1. **Watch for overly generic content and greetings**
   Cyber criminals will send a large batch of emails. Look for examples like “Dear valued customer.”
2. **Examine the entire “From” email address**
   The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.
3. **Look for urgency or demanding actions**
   “You’ve won! Click here to redeem prize,” or “We have your browser history pay now or we are telling your boss.”
4. **Carefully check all links**
   Mouse over the link and see if the links destination matches where the email implies you will be taken.
5. **Notice misspellings, incorrect grammar, and odd phrasing**
   This might be deliberate attempt to try to bypass spam filters.
6. **Check for secure websites**
   Any webpage where you enter personal information should have a url with https://. The “s” stands for secure.
7. **Don’t click on attachments right away**
   Virus containing attachments might have an intriguing message encouraging you to open them such as “Here is the Schedule I promised.”

## Speak to your Account Manager

Mitigate your cybersecurity risk during the Coronavirus pandemic

☎ 0845 345 3300

theaccessgroup.com/**cloud-hosting**