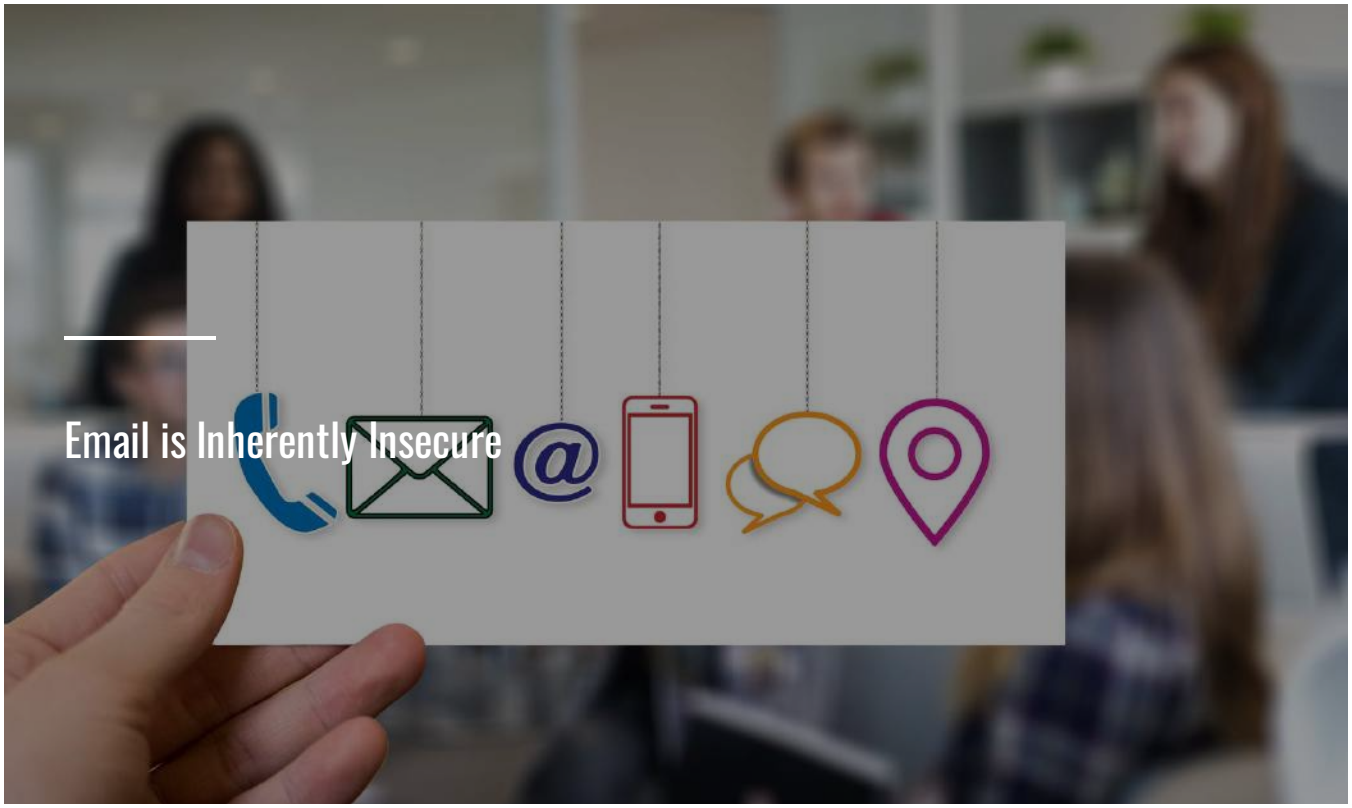
Email Security

VIGITRUST

As an employee, email most likely forms the basis of your online activity. However, used carelessly, email may provide hackers and criminals with a backdoor to enter your company's network via various methods including phishing and spoofing.
In this short course, we look at some of the common email-based security threats and what you should do to avoid them.

Email Security

Email Security



Consider this scenario. You have been tasked with creating an account for a new staff member on a key online payment processing application vital to the running of your company. The new staff member is currently working from home due to pandemic restrictions. You create the account and send a link to the application to the new employee via email.

How should you send the new employee's password?

- ◯ Include it in the email containing the link
- ◯ Send it in a separate email
- ◯ Call the new employee and provide them with their password

SUBMIT

Please answer the question before moving on

Introduction

For most individuals and employees, email forms the basis of online activity. However, email may also provide hackers and criminals with a backdoor to enter company networks through *spoofing* and *phishing* attacks (more on this later). All it takes is carelessness on behalf of one staff member to compromise the security of others or even the whole organization.

In order to prevent you or your organization falling victim to an email hack attempt, it is important that you follow email security best practice in place and know exactly what to do

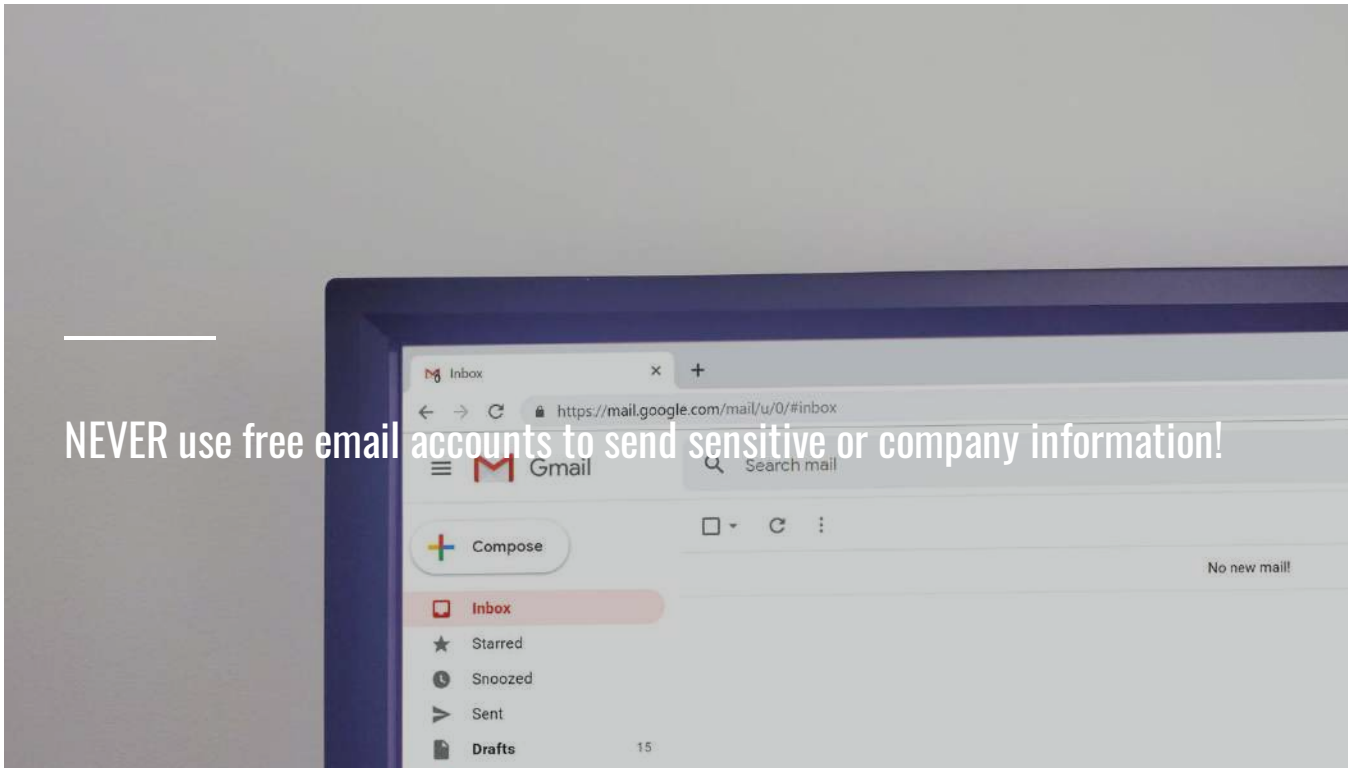
Email is Inherently Insecure

One of the first things you should bear in mind about email is that it is an inherently insecure communications medium. In addition to it forming the basis for most phishing attacks, emails can be intercepted by hackers as they travel across the Internet.

How Email is Intercepted

By default email communication is unencrypted, that is, it may be intercepted and 'read' as it travels across a network or the Internet. This is easier to do than you probably think. Hackers use widely available 'sniffer' programs that enable them to read and copy data in transit. This is why, for example, you should never send emails containing sensitive or personal data from a free WiFi hotspot, such as those found in restaurants or other public areas. These networks generally don't use encryption, so someone sitting nearby armed with a network sniffing program could read your data, or track your online activity, including online banking.

CONTINUE



NEVER use free email accounts to send sensitive or company information!

Free Email

Free email services, such as Hotmail or Gmail, don't use encryption and are generally regarded as insecure.

Another important consideration in regard to free email is the fact that you don't know where the message is stored, including any attachments, for how long, and the security controls that are applied to it.

Remember, that even if you delete an email or text message the data is not deleted from the service itself. If the data is unencrypted, it remains vulnerable to theft even if you have deleted the message.

CONTINUE

General Security Guidelines

- [ ] Remember that email is an inherently insecure medium and is open to exploitation by hackers.
- [ ] NEVER send sensitive information such as passwords or payment card details by email.

- [ ] Never click on links in emails from senders you don't know.
- [ ] Don't use free email services to send company information.
- [ ] Don't use your company email account to send personal messages.
- [ ] Write emails with due care and attention.
- [ ] Check the recipient's name before hitting the send button to avoid sending the message to the wrong person.

Tick each box before moving on

Thanks for completing this course!