

# Worried about a data breach?

As a business leader, here are 3 conversations you should be having:

## 1 ARE OUR CYBER SECURITY PROCESSES UPDATED & REVIEWED?

It's not a matter of whether a cyber security incident occurs - it's a matter of when it eventually happens... & how prepared you are.

Think of the the worst case scenario & plan for it. This may include drafting communication to affected users & government bodies. It's important to be transparent & empathetic about the incident.

You could also consider running drills to ensure your organisation has a clear process that can be executed efficiently.



## 2 HAS OUR DATA COLLECTION POLICY BEEN REVIEWED?

It's important to have robust data management policies to understand the following:

- Whose data are we collecting? E.g. Customers
- Why are we storing the data? E.g. Is it necessary to keep?
- What data are we collecting? E.g. Emails
- When are we collecting data? E.g. On activation
- Where are we storing the data? E.g. Is it on the cloud?
- How are we securing the data? E.g. What protections are in place?

## 3 IS EVERYONE AWARE OF THEIR ROLE IN CYBER SAFETY?

95% of cyber security issues are a result of human error. It's time to start talking cyber hygiene with your staff!

Educate, engage & empower your team to make better cyber safe decisions & decrease your risk of a cyber security incident.

Book a [personalised demo](#) with our team to discuss how Phriendly Phishing can help support your team's cyber security initiatives.

