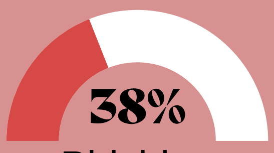
DATA PROTECTION DAY 2022

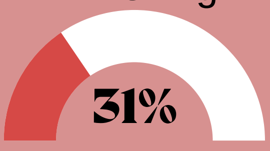
ADVENT IM

SO WHAT IS HAPPENING?

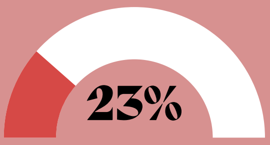
Overall, looking at the face value of the ICO figures of 2022 Q2 compared with 2021 Q2, you would think things are improving. But as you investigate further, it doesn't take long before some ugly numbers rear their heads.



Phishing



Ransomware



Data emailed to wrong recipient

One thing we noticed about the breach types is that a lot of them could have been avoided with simple **training**, low cost or even no cost interventions!

We picked out three stand out numbers here. Phishing was responsible for a whopping 38% share of all cyber breach types in 2022 Q2, with general business struggling the most from phishing, followed by ransomware at 31% and data emailed to the wrong recipient at 23%, wake up people!

These are human error, a link has been clicked or double checks have not been made. This is where training is vital.

+44%

Ransomware has DOUBLED compared to 2021 Q2 where it was up by 21% on 2020 Q2

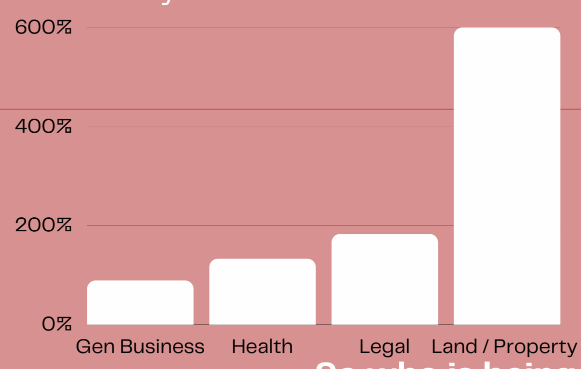
One of the stand out ransomware attacks of 2021 was the attack on **Colonial Pipeline** in late April. The attack had such large coverage as it is an important part of the national critical infrastructure system. The take down of the system resulted in disrupted gas supplies along the East Coast of the US.

Top 3 causes of Ransomware Attacks

1. Phishing Emails
2. Poor User Practice
3. Lack of Security Training

Source: Datto

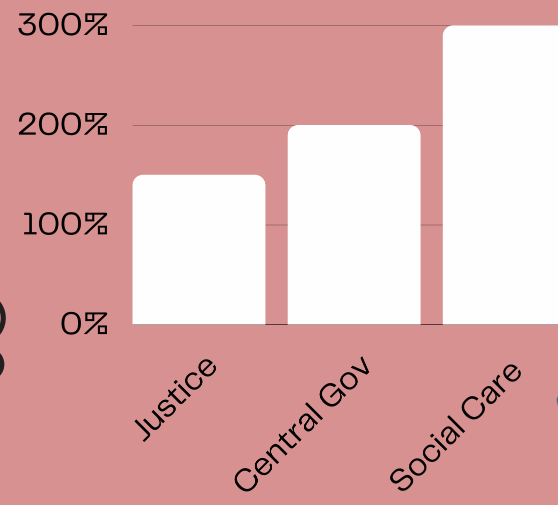
The top 3 causes of ransomware attacks prove end user education is an essential part of IT Security.



So who is being affected most by ransomware?

The above 4 sectors saw the largest increase in ransomware attacks in 2022 Q2 compared to 2021 Q2.

Loss/theft of paperwork or data left in insecure location



Shocking numbers became clear when we calculater the trend of 2022 Q2 compared with 2021 Q2, although overall both cyber and non cyber breaches are **DOWN**, there is very high levels of growth in certain sectors.

Take this example above; Justice, Central Government and Social Care all saw an incredible (bad) growth in the loss or theft of paperwork or data left in an insecure location.

So what actually causes that? Overwhelmed staff, lack of training or poor practice?

Well it could be any of those things, but they are all human error or misjudgement.

How to avoid or minimise the impact of ransomware;

- Train your staff to raise the alarm to the security team
- Regularly back up your data
- Develop plans and policies
- Keep systems up-to-date
- Have a comprehensive business continuity plan

Where does training come into this?

Having a strong security culture will protect your organisation against cyber and non-cyber threats and possible data breaches. Keep in mind the average cost of a data breach, as well as a financial loss, this could also result in a loss of business projects, vulnerability to future attacks and a damaged reputation. Remember, the cost of a breach, both in financial terms, time and reputational damage will far outweigh the cost of training your staff.

#DPD2022

References Information Comissioner's Office

advent-im.co.uk