LOCKDOWN

When was the last time you changed your email password? If it wasn't yesterday it may be too late. With so much data on the move, the question may be when is that data going to end up in the wrong hands

IN 2011, GOOGLE WAS FINED EUR100,000 IN FRANCE FOR the unauthorised collection of personal data for its Street View mapping service, the heaviest penalty levied by an EU regulator to date for breaching privacy. Meanwhile, authorities in South Korea, New Zealand, the UK, Canada and Spain found that Google's wi-fi interception violated applicable laws. Google was fined US$25,000 for impeding a US investigation into the same issue.

It seems that the camera-equipped cars the search giant uses to take pictures for Street View inadvertently collected personal data from unsecured wireless networks across the world over a period of years. And Google didn't notice. Or hoped no-one else did.

In the last eighteen months in the UK public sector alone, organisations including NHS bodies, police and local authorities have received fines in excess of GBP 2 million for serious breaches of the Data Protection Act.

If this isn't enough to set alarm bells ringing, consider that the US doesn't have comprehensive privacy and data protection laws, relying instead on a mix of legislation, regulation and self-regulation. This is the nation with the world's largest Facebook population, with 167,431,700 users, according to Social Bakers. The sea of available information is mighty deep and there are no lifeguards.

Before the internet, we locked our paperwork in safes, which safeguarded our intimate secrets and identities. Not today. In the information age, so much of what we could once lock away has taken on more ephemeral hues. Our liquid assets are numbers on a screen and the details of our lives are owned by social networking sites.

Walid Kamal, senior vice president technology security, risk and fraud management at du, suggests we should be aware of the information we put out there. "Identity theft is the fastest-growing cybercrime," he says. "The type of personal information we store on the web and in our smartphones, such as names, phone numbers, home addresses, occupations, postal codes and marital statuses, are probed, stolen and manipulated by identity thieves that use the records to apply for credit cards, loans and home mortgages."

Recent statistics show some 15 million people annually fall victim to identity theft in the US alone, with financial losses totalling a staggering $50 billion.

In 2012, The Norton Cybercrime Report announced that cybercrime is bigger than the drugs trade. The financial cost of cyber attacks worldwide is estimated at $114 billion, with time lost dealing with the crime adding another $274 billion. The criminal costs are higher, yet the costs of committing the crimes are much, much lower.

Ultimately, it is not enough to keep an antivirus programme up-to-date, decline cookies and never answer emails from anyone from the Ivory Coast keen to make you a millionaire. The Cybercrime Report concludes that despite 74 percent of people being aware of cybercrime, 41 percent don't have up-to-date security software and 61 percent don't use complex, regularly-changing passwords.

"When we send an email using public email providers, or when we transmit corporate data over the internet so it can be stored in cloud storage providers, we 'allow' that information to be possibly intercepted, copied, disclosed, manipulated, deleted and altered," Kamal explains.

On smartphones, security measures are close to non-existent. Many rely on a four digit pin code set to "0000". The major players have developed mobile security programmes but they don't come as standard. The phone is a data-mining paradise. It is not easy to hack into a phone – but it can be done.

As technology advances, so do opportunities. Applications exist that allow you to unlock your car from your phone, your credit card details are stored on eBay, and in Japan it's common to use a phone to pay for goods from vending machines. All innocuous activities until they're hacked.

Move from the personal to the corporate and cybercrime becomes more serious. Breaches of privacy and unsecured data provide an "in" for corporate crime. Banks, phone companies and big financial players pay big bucks to security experts for a reason. The least we can do is change our passwords regularly.

THE SEA OF AVAILABLE INFORMATION IS MIGHTY DEEP AND THERE ARE NO LIFEGUARDS

WORDS GISELLE WHITEAKER

Image: Shutterstock.com