

THE CASE FOR EMAILING... DIFFERENTLY

Most of us recognise the online risks, and as many as half of us have been hacked... and still we do nothing.

stayprivate.com

THE CASE FOR EMAILING... DIFFERENTLY

Most of us recognise the online risks, and as many as half of us have been hacked... and still we do nothing.

Nothing ever changes... right up to the point when it then does.

Yes, on one level, blindingly obvious. But less obvious or predictable is what it actually takes for change to occur? How do you get to the tipping point? Where the dam breaks. Where opinion and influence extends to the point of action on the part of one, that then ripples to 'The Many'.

How do people change their behaviours? Just what does it take?

The plain and cold truth of it is that CHANGE (behavioural, social, cultural) can be tricky to bring about. Because none of us are huge fans of it. Instinctively, we perceive change as something unruly and precarious. Words like familiar and predictable make us feel safe and centred. They're soothing to the ear. They may even slow our heart rate a touch. The familiar is a cosy blanket. Whereas 'change' is a groan and grimace.

Change implies hassle and inconvenience. And change's bedfellow, 'Uncertainty', positively brings on palpitations. Uncertainty might be good for newspapers sales, but it's the kind of cortisol spike most of us instinctively cross the street to avoid.

So what does it take to convince us all of the need for bona fide change? Perhaps it's the presenting of unshakable facts, newly brought to light? Perhaps it's personal, first-person experience? Whether first or third-person, it has to be a damning critique of today's normal, in order for us all to embrace a New Normal.

We recently commissioned a research study into online behaviours and perceptions of safety. Very simply, going into 2018, we wanted to take a temperature read on where people's attitudes and behaviours are at.

- How safe do people feel online, and how prone do they feel to cyber threats?

“——
What does it
take to
convince us all
of the need for
bona fide
change?
We recently
commissioned
a study into
online
behaviours and
perceptions of
safety.

——”

THE CASE FOR EMAILING... DIFFERENTLY

- When it comes to email usage, for example, do people feel they can communicate safely?
- Or do people, and indeed businesses, recognise the threats and are they starting to act differently?

Some of the key findings can be boiled down, as below, into 3 HEADLINES and 5 BULLETS:

AWARENESS OF THE RISKS IS NOT A PROBLEM

1. 87% of the British public **ACKNOWLEDGE** that their personal and confidential information is at **RISK** when stored and communicated via **UNSECURE WEBMAIL** platforms like Gmail, Hotmail and Outlook.
2. 73% of business owners and C-Suite's **RECOGNISE** that using their clients' personal email for sending and receiving personal and confidential information makes them **cybercrime TARGETS**.

THE PROBLEM IS PROMPTING PEOPLE TO DO SOMETHING ABOUT IT

3. 50% of people who've been hacked **CONTINUE** to send personal and confidential information via personal web based email accounts (such as Gmail, Hotmail and Outlook).

THE CURRENT CLIMATE IS ONE OF CONCERN BUT INACTION

4. 1 in 3 businesses are **WORRIED** that cybercrime is becoming more of a threat to their business.
5. 46% of businesses **SUSPECT** that they are likely to be a future victim of cybercrime.

(Source: Atomik Research Group. Research published: Q1 2018. Conducted: 2017. Research sample A: 2,006 UK adults. Interview sample B: 202 C-Suite & Company Founders.)

“
Awareness of
the risks we
face online is
not the
problem.
The problem
is prompting
people to do
something
about it.
Our current
mind-set
remains one of
concern but
inaction.

”

THE CASE FOR EMAILING... DIFFERENTLY

Sometimes the facts speak for themselves. And sometimes they still fall on deaf ears.

What's fascinating is how the above 5 statistics reveal our human condition, our current inaction to online dangers, and the speed at which we begrudgingly consider changing our ways.

50% of people who have been hacked STILL continue to use unsafe, unencrypted webmail platforms. Three-quarters of business acknowledge the likes of Gmail isn't safe, and STILL send emails to their client's Gmail account. How burned do any of us have to get before we act differently?

Forbes recently reported the estimated cost of cybercrime at approximately \$6 trillion per year (on average through 2021).

Accenture's 2017 'Cost of Cybercrime' study reported a 27.4% net increase in the "average annual number of security breaches". It did however also report that companies are starting to respond, spending 23% more year-on-year on security technologies to counter the growing threats from hackers and malware.

Typically, something has to properly happen, to consequently drag us out of our default state of indifference and denial. "Implicit threat" is often not enough for us to act differently

It's not a criticism of the human condition, just a reality of it. We human beings can be a little bit recklessness and 'chance our arm'. Not so much so that we made ourselves something else's lunch, but it could certainly be argued that we've evolved to such an extent that we don't now still recognise threat as well as we should. Our actions and inactions could even have something to do with how we're cognitively wired.

The survival function in our brain is little different to the animals from which we evolved. Our Fight/Flight/Freeze mechanism originates in the amygdala (the bit shaped like an almond).

“——
50% of people
who've been
hacked STILL
continue to use
unsafe,
unencrypted
webmail
platforms.
Three-quarters
of businesses
acknowledge
Gmail isn't
safe, and STILL
send emails to
their client's
Gmail account.

——”

THE CASE FOR EMAILING... DIFFERENTLY

The moment we perceive a potential danger, our amygdala immediately flicks the switch. Whereas the 'thinking part' of our brain, responsible for judgment and values, has nothing to do with the amygdala. Reason and rational thought lives in the Prefrontal Cortex. When our amygdala talks to us, we act fast. When our Prefrontal Cortex does the talking, we do exactly as our ever-civilised selves would do. We tend to think about it some more, and weigh the pros and cons.

Something as seemingly simple as how we email exposes an 'Old Brand-New Brain' dilemma.

In just the same way that we shy from change, the case could be made that our 'Modern World' has dulled our survival instincts, and that the Online World is currently our major blind spot. We face the contradiction of being Apex Predators with Gmail accounts and a predilection for over-thinking the increasingly obvious.

Knowing what we know, the question remains.

When do we all start doing something about it?

ABOUT US

StayPrivate ensures safe and secure 2-way communication between businesses and external contacts. Our plug-and-play solution is compatible with all email accounts, making it incredibly easy to encrypt emails and share files securely.

With click-and-PIN access, TLS connections, AES-256 encryption and multi-factor authentication, StayPrivate enables companies of any size to send and receive personal data in a GDPR-compliant manner.

GET IN TOUCH

+44 (0) 20 7101 5000 | sales@stayprivate.com | www.stayprivate.com

“
How we email
exposes an 'Old
Brand-New
Brain' dilemma.
Our 'Modern
World' has
dulled our
survival
instincts, and
our 'Online
World' is a
major blind
spot. We're
Apex Predators
with Gmail
accounts and a
predilection for
over-thinking
the increasingly
obvious.

”