CSS PLATINUM

# Monthly Security Newsletter.

## Welcome to the summer season edition!

Many of us are currently enjoying the summer season; however, keeping safe whilst away is always a priority. On page 2, we provide a checklist of security measures to ensure your guest have a sunny yet safe trip away!

We are delighted to announce that the CSS Platinum team will attend the Cannes Yachting Festival and Monaco Yacht Show in September!

With a brief to bring super yachting to a new generation of clients, we are excited to discuss all things cyber security!


As featured in:

**GIBRALTAR INSIGHT**

June 22 Issue

## Are you Cyber Resilient? ...Are you sure? ...How do you know? and what should you do about it?

Cyber-attacks are a modern-day plague on society. They impact businesses, people, and us all in one way or another. Frighteningly, it also funds international crime and global terrorism. Cybercrime causes significant impact and distress to you and others, either knowingly or unknowingly

Cyber Criminals target the weakest prey. They are motivated by two things: money and freedom, aka: "not getting caught." Unless you have something that a cyber-criminal wants at all costs, the harder you are to hack, the more likely they will go elsewhere. So their plan is simple: minimum effort for maximum reward from as many people or businesses as possible.

You may consider that your business is doing all the right things. But are you sure? How do you know? Who is providing your advice? Is your advisor a qualified cyber expert? Are you tracking up-to-the-minute cyber threats? Do you know what is happening at this very minute that may affect your networks, mobile applications, web portals and collaboration tools?

We often hear, "yes, we have addressed cyber security, we have anti-malware, firewalls, VPNs and have conducted a penetration test 3 years ago and a 45-minute training package." All of this is positive, but it is probably only at the absolute minimum level that must be considered relative to modern threats.

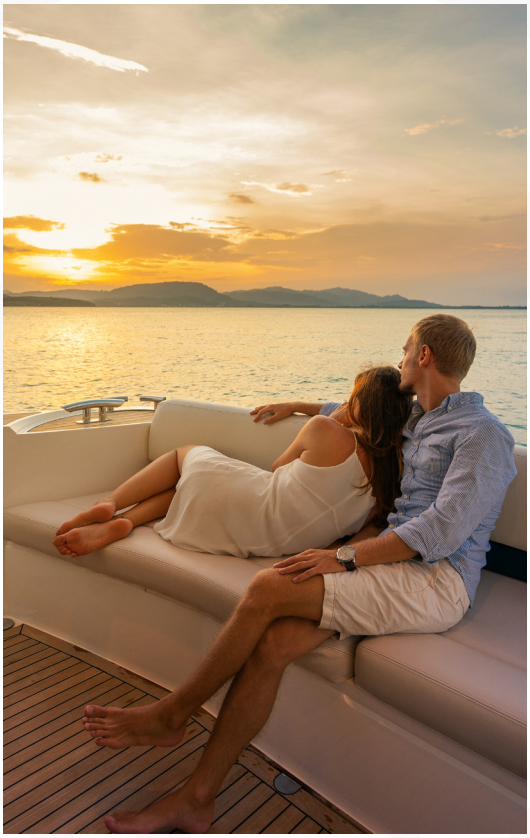
Read the full article on the CSS Platinum website by clicking here.

CSS PLATINUM

# Monthly Security Newsletter.

## Holiday Security Checklist:

## Your home alarm is activated but have you (or your guests) done the same for your online security?



The fact is that cybercriminals will be looking to exploit holidaymakers during the vacation season.

Whether staying local or heading abroad, people tend to put themselves at risk while on holiday without realizing it. Social media is a great way to connect and share with people, but you must be aware that your friends and family may not be the only ones viewing your posts.

### How would Cybercriminals use your social media to target you or your guests?

Cybercriminals actively use social media for opportunity and intelligence gathering – whether to find individuals to target or bolster information to enable them to socially engineer an attack. While the information in isolation does not amount to much, cybercriminals are experts in combining pieces of data to become intelligence to target someone.

People post all kinds of information on social media: email addresses, mobile numbers, addresses and more. Also, pictures and videos of luxury assets, expensive cars, jewellery, or just the fact you are away from your home all builds intelligence on you and your close ones.

### How to protect yourself:

- Start by **turning on privacy settings for all your social media accounts**. You would hope that the privacy settings are turned on by default for whatever social media platform you choose to use. Unfortunately, they rarely are, and this can mean that anything you post – photos, videos, or locations – could be seen by anybody with an account for the platform.
- The information for how to do this for each platform is readily available on Google but, of course, this only controls what you post, so it is worth **setting boundaries with friends and family over what they post regarding you** – particularly if their privacy settings aren't up to scratch.
- **Avoid tagging your location in real-time**. If someone is watching, they can easily see you are not at home or in a particular place wearing an expensive piece of jewellery, for example.
- Using **strong passwords** is a critical cyber resilience practice. Doing so means cybercriminals are unlikely to gain unauthorized access to your account, which could enable them to change your privacy settings or gather information for social engineering purposes.
- **Never use the same password across multiple accounts**. If one site is breached and your credentials are exposed, your risk is amplified exponentially if you use that same password across multiple other accounts.
- **Turn on two-factor authentication**. This will let you know whether someone is trying to access your account and take appropriate action.