a window into cyber

a note from Ben Maidment

We're lucky we have the technology today that enables us to adapt as much as we can to the world we currently live in. But while we adapt to this brave new world online, so too, are the new crop of cyber threats we face. As we shift to spend more time in front our computer screens, we open ourselves up to more technological risks and privacy issues.

So it's important we learn how best to protect ourselves against the advancements of this new cyber landscape. It seems an apt time, then, for this to be the first edition of *A Window into Cyber*.

In our inaugural issue, we explore the ins and outs of ethical hacking with FreakyClown and provide an underwriter's tips for securing your WFH office.

At Brit, we're here to help build a more secure future by providing our policyholders with proactive features like Datasafe. We hope our newsletter becomes a source of knowledge that aids you on your continuous journey of cyber literacy. In these unprecedented times, let's do what we can to stay connected.

this month's author: FreakyClown

Co-CEO and Head of Ethical Hacking, Cygenta   @_freakyclown_

FC has worked in the Information Security field for over 20 years as an ethical hacker and social engineer. He performs valuable research into vulnerabilities, 'breaking into' hundreds of global banks, offices and government facilities to demonstrate weaknesses in physical, personnel and digital controls, and help organisations improve their security. As former Head of Cyber Research at Raytheon Missile Systems, FC has collaborated with intelligence agencies and assisted governments against national security threats.

the hacker mindset

by FreakyClown | Read time: 4 minutes

When George Mallory was asked why he set out to climb Everest he famously uttered the phrase, "Because it's there." It sounds like such a carefree and even condescending way to answer, but it's often misunderstood. He wasn't being dismissive, but instead he was showing there was nothing else really left in his life; he had just returned from war and found much of his life missing or no longer how he expected it. The mountain, therefore, gave Mallory a focus, a reason and more importantly, hope for a life worth continuing to live.

Hackers have a peculiar mindset, and as many children in playgrounds around the world will often call out – it takes one to know one. I am a hacker and I have been since I was also running around playgrounds. I am, however, not a criminal, nor have I ever been. I have been working as an ethical hacker for decades and now lead ethical hacking for Cygenta, the company which I co-founded and of which I am co-CEO.
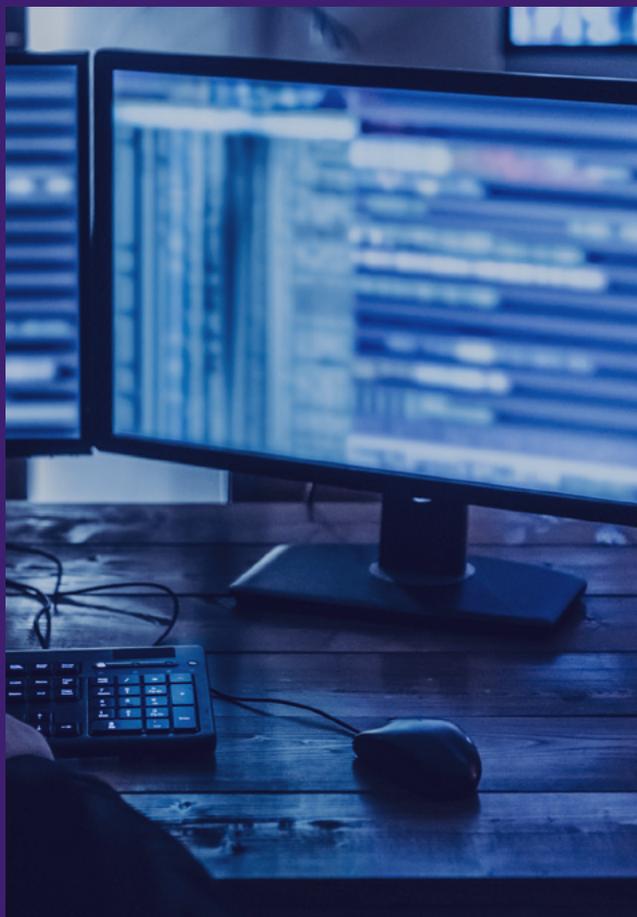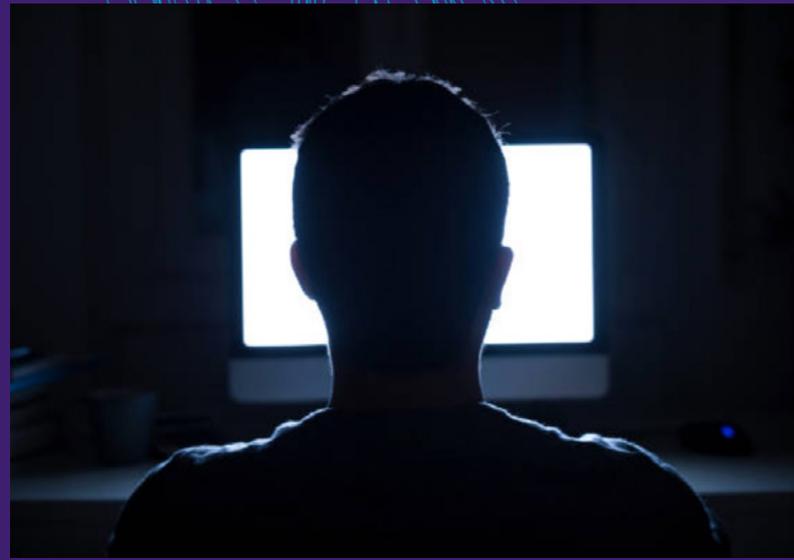
I am a hacker and I have been since I was also running around playgrounds. I am, however, not a criminal, nor have I ever been.

Hackers are a rare breed of people that often obsess over a problem or see patterns much more than the average person. We often, at least when starting, have little direction or focus in life and the cold hard logic of computer systems can appear friendly and easy to understand. Many of us lack the social skills to interact with others around us, which means that communication over IRC or Twitter is easier than face to face. Since the social lockdown enforced on the world by the COVID-19 pandemic, hackers have been happier because the countless hours we spend working with computers rather than going out to pubs or clubs no longer makes us seem weird, but socially responsible. Whilst some of the tropes of the hacker are real, the one that proposes criminal hackers are just hacking because they are bored can now be put to rest. With the lockdown in place and boredom at an all-time high, we were expecting a large uptick in attempted hacks. Thankfully we have not seen this, but there have been other interesting changes in criminal activity.

At the beginning of the year, I was fortunate enough to present a talk on criminal hacking to the clients and customers of Brit Insurance and demonstrate some of the tools and methods used by them. One of the interesting things that we noticed at this time was the drop in the number of nation state attacks. Unfortunately, these have since risen beyond the levels of individual criminal hacks. This gives us a good insight to the mind of a criminal attacker: that they see hacking as more of a job than something driven by boredom, and that they are the antithesis of the ethical hacker who is driven by a desire to make things more secure.

Society has changed incredibly over the last couple of generations. I still remember the security innocence that we had when the World Wide Web was born. No one could have predicted where we would be today! The first computer systems didn't have or need passwords. Access was based on trust –something unimaginable today. We piled system after system on top of a poorly laid out foundation, leaving almost everything vulnerable to attack today. I recently suggested in a roundtable with the United States government that they scrap the whole thing and start again, and not so surprisingly, many people in the room agreed.

Hacking is more than just a job. It's a hobby and a lifestyle; but most importantly, it's a mindset.

Hacking is not always a crime and not all hackers are criminals; hacking can be used for good as well as bad. Hackers are technologists that understand the foundations of technology well enough to be able to manipulate it in such a way as to enable unintended access or cause unintended consequences. Ethical hackers such as myself help organisations secure themselves against cybercrime by exposing the vulnerabilities in systems so they can be fixed before they are exploited. Hacking is more than just a job. It's a hobby and a lifestyle; but most importantly, it's a mindset. When faced with the problem of how to manipulate or subvert a system, I will often describe it as an "itch inside my head that I must scratch."

So, why do hackers hack computers? Because they are there!
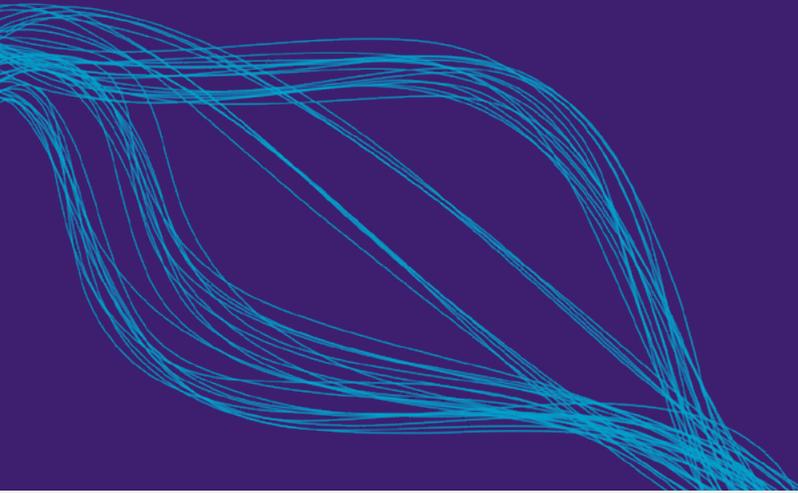
an underwriter's outlook

top 5 tips for SMEs with employees

shifting to working from home

Adelle Gruber, Senior Underwriter, Cyber | Read time: 5 minutes

Over the last month, the UK's businesses, large and small, have been at the sharp end of adapting to the new normal of the coronavirus (COVID-19) situation. As part of this, to help manage the virus' spread, many organisations are mandating that their staff work from home.

Whilst COVID-19 may have precipitated a sudden uptick in remote working, it is merely a catalyst of an already growing trend. A 2019 study by International Workplace Group, found that 50% of employees work away from their office at least 2.5 days per week.

[click to read full article in SME Technology Guide](#)

highlights from Datasafe

BRIT

Datasafe delivers the latest risk management resources so clients can proactively manage their data protection and privacy risk.

higher than average usage this month included:

573
pages viewed

258
logins

540
online training courses completed

top training courses completed:

Phishing

Spear-Phishing

Malware

Password Best Practices

Public Wi-Fi

COVID-19 now on the Knowledge Center:

With the recent shift to remote workforces, Datasafe continued to focus on ensuring Brit policyholders know that remote workers need the same (if not more) level of attention to cybersecurity as if they're working in the office. To help policyholders remain vigilant during this challenging time, Datasafe launched a COVID-19 section on the Knowledge Center featuring:

Comprehensive guide on How to Securely Work from Home

Working from Home: Quick Tips

Guidance on Using Zoom Securely

Alerts regarding coronavirus phishing emails, stimulus scams, and tips for detecting other COVID-19 scams

Thursday, 5/21/2020
10:30 AM PT/1:30 PM ET

Post-Ransomware Attack Webinar

Navigating the aftermath of a ransomeware attack is vital to the long-term viability of your business. Join Datasafe's free webinar to learn best practices in an interactive session so you have an action plan ready.

register now

britinsurance.com/cyber