k3 cloud, hosted and managed services

HALLOWEEN HACKING HORROR STORIES

AND OTHER IT SECURITY NIGHTMARES FROM THE 'K3 KRYPT'

Have you ever dared to wonder what would happen if your technology fell into the wrong hands? Hacks, breaches and leaks truly are the stuff of nightmares – and to make matters worse, they're more common than you'd like to believe.

To give you a fright this Halloween, we've dug up some of the most bone-chilling, blood-curdling and altogether petrifying cybersecurity horror stories from recent years. Read on at your peril!

THE NAIL IN THE COFFIN

The ill-fated Google Plus actually said its goodbyes 4 months earlier than planned. And why did it head to the social media graveyard prematurely? Due to a huge leak affecting the personal data of half a million people! To make matters even more horrifying, a second security breach went on to impact a huge 52 million users – sealing Google Plus' fate once and for all.

THE HOLIDAY (BOOKING) FROM HELL

500,000 British Airways customers faced a living nightmare when their data was compromised as a result of a sophisticated scam. Using clever trickery, cybercriminals lured unsuspecting BA customers into a trap (in this case, a fake website with fraudulent data capture) to harvest their details. The airline faced a hair-raising £183m fine as a result!

PARANORMAL PROJECT MANAGEMENT

Due to administrative error, the UK government could have found some unwelcome guests sneaking in the shadows of the parliamentary labyrinth. Confidential documents detailing how to gain access to government buildings were temporarily posted to Trello (a web-based project management tool) and visible via Google search. An omen for the digital age if we ever heard one!

MORE TRICK THAN TREAT

Europe's largest manufacturer of wires and electrical cables suffered a shock when a whaling attack tricked finance staff into transferring a bone-chilling £34m into a false bank account. By hacking into systems and creeping around private data, cyberattackers were able to effectively mimic a top executive and make a convincing transaction request.

THE DEMONIC DATA BREACH

Popular ride-hailing app Uber received the fright of its life when the data of 50 million customer accounts was stolen by some sinister cyberattackers. The company paid an arm and a leg (£81,160) in return for the breached data to be deleted from the cybercriminals' systems.

A MENACING MALWARE MYSTERY

In a spooky unsolved mystery, an entire Alaskan borough was cyberattacked leaving its businesses and domestic communities without access to any sort of computer networks. A whole array of services were downed – including libraries, animal shelters and government facilities - along with data being permanently lost. To this day, the borough still doesn't know who (or what) was responsible – chilling stuff!

HAUNTING ON THE HIGHWAYS

As part of an eerie experiment, professional hackers remotely toyed with the controls of a Jeep Cherokee - while it was being driven by a real person! During the alarming ordeal, they tampered with air-con, radio and windshield wipers - and then cut the engine. The Jeep was paralysed on a busy interstate, and with an 18-wheeler truck coming up fast from behind. Luckily, the digital carjacking stopped there.

If you're feeling the cold ghostly hand of Halloween IT Security on your shoulder, then fear not. Our Halloween hacker hunters have created a quick and easy way for you to assess your own IT security situation.

Download and complete our interactive PDF scorecard to get your personalised IT security score!

k3starcom.k3btg.com | 0844 579 0800