Different Types Of Hackers – And What They Mean For Your Business

Bridewell Consulting - October 1, 2018 - The Bridewell of Knowledge

In the past, we've talked a lot about our security services and how thoroughly we can test your business for cyber weaknesses. One of the terms we used in that was 'White Hat Hacker', to describe ourselves. Now it might seem odd to refer to a high-level cyber security company as 'hackers' but, that's exactly what we do only, we aren't on the 'dark side'. While the media might do a good job of making all hackers out to be these malicious people who meet after dark and conspire to steal from innocent businesses, the reality is that there are lots of different kinds of hacker out there. Each one with their own motives, skills and plans for your business. The types of hacker are often referred to as wearing different coloured 'hats', with each one having a different implication for the target. To illustrate, here's a list of what each kind of hacker does, and what that might mean for your business.

Black Hat

The stereotypical 'hacker' – the kind you hear about on the news.

Motives: Financial gain.

Aims: To break into your business and steal bank details, money or confidential data. They usually use these stolen resources for their own gain, to sell on to the black market or to extort the target business.

What That Means for You: Black Hat hackers are at the top of the business risk list. Their methods are varied but basic, so they can be protected against. But if their attacks are successful, the results could be devastating for your business and your customers.

White Hat

The Yang to the Black Hat's Yin, White Hat hackers are the polar opposite of the Black Hat in every way.

Motives: A desire to help businesses, along with a passion for finding holes in security networks.

Search

RECENT POSTS

DCR Magazine: Bridewell Consulting predicts top six cybersecurity trends in 2021

Optimising Data Security

Using ORCA to improve your email defences

PCI DSS – Remaining compliant between assessments

We invest in people, silver accreditation

CATEGORIES

Exhibitions

Fun

Newsroom

Recruitment

The Bridewell of Knowledge

Uncategorized

ARCHIVES

Select Month

Aims: To protect businesses and support them in the ongoing battle against cyber threats. A White Hat hacker is someone like us – a company or individual who will help you protect your business. They can help you put effective protections in place, find vulnerabilities and provide solutions to solve them, before other hackers find them. There is even a qualification and organisation specifically for them – the CEH (Certified Ethical Hacker) from the EC Council.

What That Means for You: A business that is well protected from every angle of attack in the digital world, and ongoing support in case of a breach.

Grey Hat

Nothing in life is black and white, and neither is hacking.

Motives: Personal enjoyment.

Aims: Grey Hat hackers have all the skills of a Black and a White Hat hacker. The difference is, they don't care about stealing from people, nor do they particularly want to help people. Instead, they like to play with systems and enjoy the challenge of finding gaps, breaking protections and generally just find hacking fun.

What That Means for You: Despite their skill set and the fact that they do break into systems, Grey Hat hackers will rarely do anything harmful. They break into things because they can, and then move on. Grey Hat hackers actually make up the majority of the hacking community, even though it's the Black Hat's most people know about.

Blue Hat

Vengeful and aggressive in every way- but only if you create them.

Motives: Revenge.

Aims: Blue Hat hackers often take existing code for malware and viruses they find online, then modify it to meet their needs. They will use this code to target the business or individual they feel has wronged them and inflict their revenge.

What That Means for You: Generally, only a problem if you've made someone very, very angry. This could be a customer, supplier or employee – anyone who might be so angry that they want to 'make you pay'.

Red Hat

The caped crusaders of the cyber world.

Motives: Vigilante justice.

Aims: To put a stop to people they know to be Black Hat hackers. But they are downright scary in how they go about it. They essentially take the Black Hat's arsenal and turn it back against them. Using malware, DoS attacks, viruses and Trojan Horses to destroy their machines from the inside out. It's a pretty effective way of stopping them from attacking anyone else!

What That Means for You: Nothing really. Red Hat hackers are similar to White Hat ones, in the sense that they are working to put a stop to Black Hat attacks on your business. But you probably won't know about it.

Green Hat

Baby hackers taking their first steps in the cyber world.

Motives: Learning to be full blown hackers.

Aims: Green Hat hackers are all about the learning. They are new to the world of scripting, coding and hacking in general, so you probably won't find one attacking. Instead, they hang around online message boards asking questions of more developed hackers, honing their skills.

What That Means for You: Green Hat hackers don't really represent a threat to businesses. They are still 'green', and more interested in learning *how* to hack than actually doing it.

Script Kiddie

This is something of an 'odd one out', since it's neither a hat or a colour! But a Script Kiddie can still cause problems, no matter how innocent the name sounds.

Motives: Causing chaos and disruption.

Aims: Script Kiddies have no interest in things as mundane as theft. Or, as it turns out, script. They don't tend to develop their own software – instead they download existing malware development software and watch videos on how to use it. When they're confident, they'll attack. A typical Script Kiddie attack would be a DoS (Denial of Service) or DDoS (Distributed Denial of Service). This basically means they flood an IP address with so much useless traffic that it collapses. Think most retail websites on Black Friday. It causes chaos and prevents anyone else from using the service.

What That Means for You: While they might not present a financial risk, Script Kiddies can be a pain. They can cause disruption to your business that can damage your reputation or lose you customers, and it can take some time to get everything back online afterwards.

So hopefully that clears a few things up and gives you a bit of an insight into the world of hacking in all its colour! At Bridewell, our job as White Hat hackers is to keep all of the other hackers out of your business by identifying weaknesses; protecting you, your clients and your data. For more information or to enquire about out security testing process, get in touch with us today.

TAGS: CYBER SECURITY, HACKERS

PLEASE SHARE THIS

← Previous Post
10 Ways GDPR Will Impact Your Business Operations – Part 1

Next Post →
What Is Cyber Security?

YOU MIGHT ALSO LIKE

June Webinars
May 28, 2020

The IASME Partnership
April 1, 2020

We invest in people, silver accreditation
November 20, 2020

CONNECT WITH US

Email: bc@bridewellconsulting.com **Twitter:** @BWC_Security **Phone:** +44 (0) 3303 110 940

Address: 40 Caversham Road, Reading, RG1 7EB
Company registration number: 11101195 registered in England & Wales