
space∞
HACKING
FOR GOOD

# CHAPTER 1

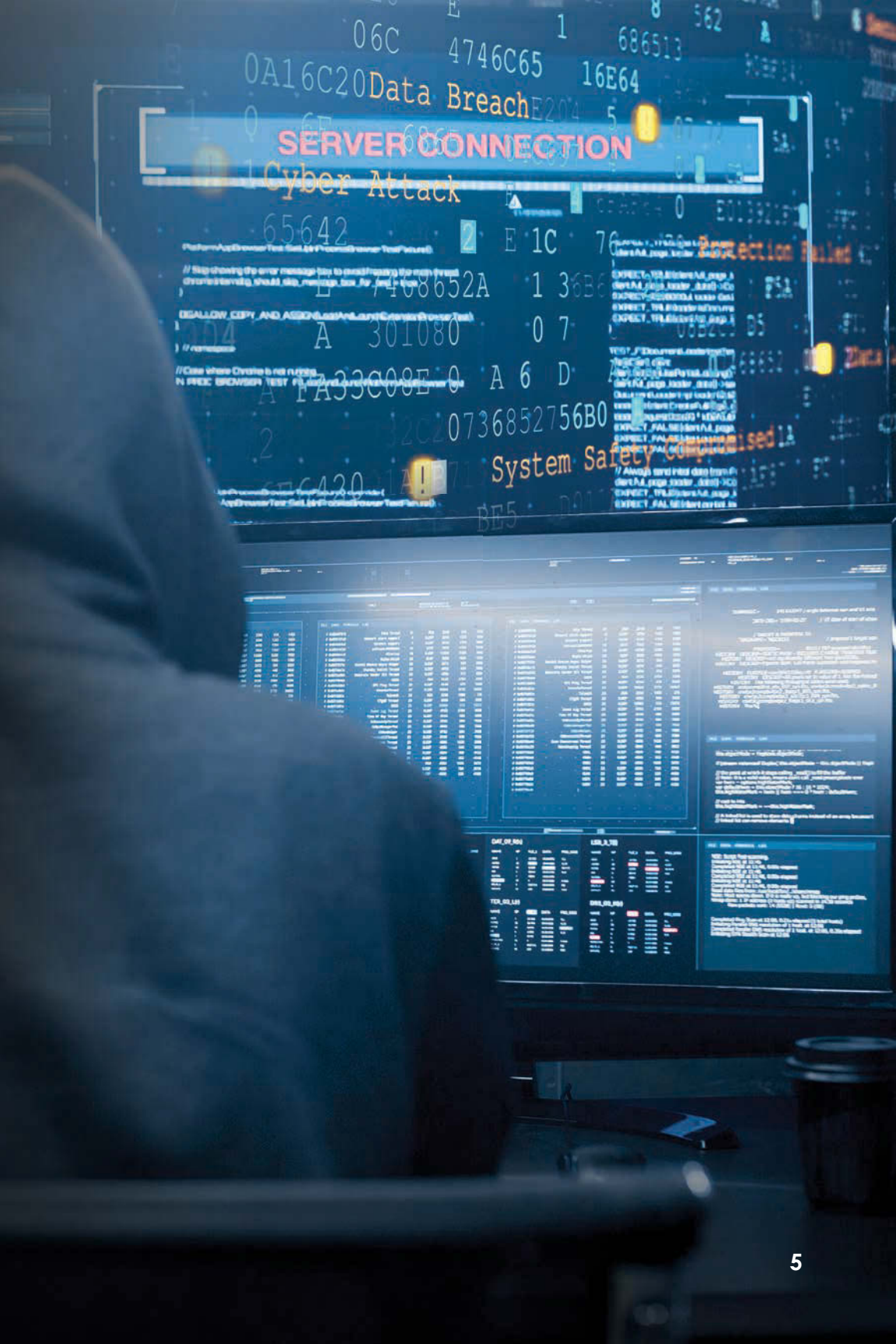
## WHITE, BLACK, AND GRAY HATS

Computers are an important part of our lives. They are used in schools. Stores and restaurants have them too. Pilots use them to fly planes. Some surgeons use computers to operate. Businesses rely on them for communication. People depend on computers. But these machines have weaknesses. They can be **hacked**.

Big news broke in 2016. Yahoo is a major search engine. It is also an email provider. The company had been hacked. This had happened three years earlier. People were just finding out.

Yahoo had three billion users. All were affected. Hackers stole names and email addresses. Passwords were also taken.

This hack showed that even big tech companies are at risk. Their users are too. All hackers look for one thing. They want to find holes in a computer system. These holes let them break in.


Data Breach
SERVER CONNECTION
Cyber Attack
System Safety

Not all hackers are bad. In old western movies, good guys wore white hats. Bad guys wore black hats. These terms are now used for hackers.

"White hat" hackers use their skills for good. They look for weaknesses. Then these hackers fix them.

"Black hat" hackers commit crimes. They may steal. Some take money. Others go after information.

There are also "gray hats." They are a mix of good and bad. Some might find a gap in a company's security. Then they tell the company about it. But gray hats often want money in exchange. Without payment, they may put the information online. Then anyone could use it to hack in.

Gray hats can also be whistle-blowers. They tell the public about bad practices. These might include spying or hacking. The government may do this. Companies might too. Whistle-blowing is often protected by law. But it can be illegal. It could risk national security. Still, many think whistle-blowers are doing the right thing.

Many white hat hackers work in **cybersecurity**. Companies need to test their computer systems. White hats are hired to do this. These workers think like black hats. How would a black hat get in? What would they look for? They figure out how to protect against them.

Some white hats just enjoy solving puzzles. Hacker **conventions** hold contests. Many are open to both kids and adults. People compete to hack websites. They can hack devices too. Software gets tested in a safe place.

## EARLY WHITE HATS

After witnessing the aftermath of one of the first internet bugs in 1988, computer science student Dan Farmer decided to specialize in security. With the help of Wietse Venema, another security expert, Farmer showed that cyberattacks could happen in different ways. The pair also offered tips on how to protect computer systems.

Farmer and Venema created an important tool and released it as free software in 1995. It was called SATAN. This stood for Security Administrator Tool for Analyzing Networks. SATAN could scan computers and show the possible risks and how to fix them. Companies could then test their own systems.