Internet Security

About hackers, spam, threat identities

Internet Security

Internet security is a branch of computer security. It encompasses the Internet, browser security, web site security, and network security as it applies to other applications or operating systems as a whole.

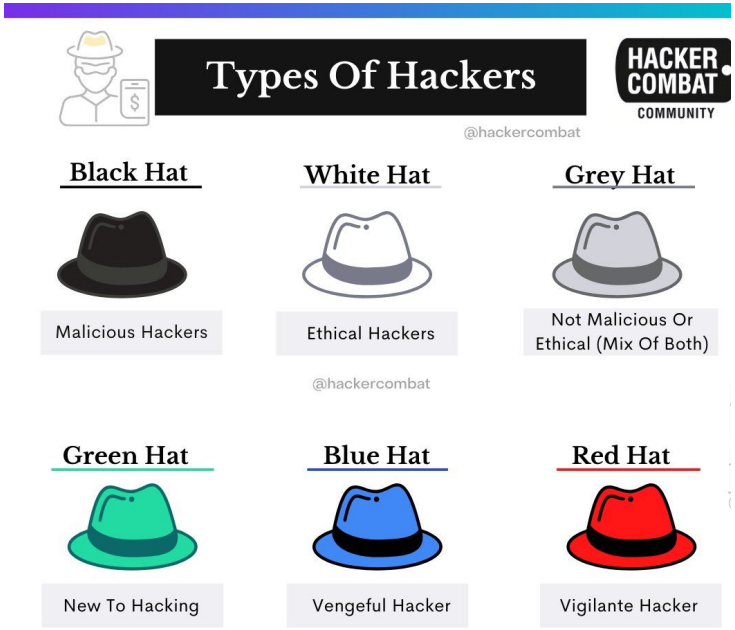
Its objective is to establish rules and measures to use against attacks over the Internet.

The Internet is an inherently insecure channel for information exchange, with high risk of intrusion or fraud, such as phishing, online viruses, trojans, ransomware and worms.

Many methods are used to combat these threats, including encryption and ground-up engineering.

Hackers

A hacker is anyone who is well-versed in the weaknesses of computer programs and understands the depths of computer systems.



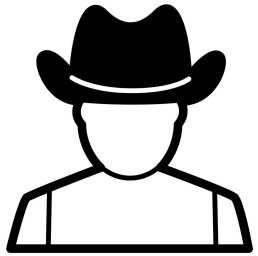
The most dangerous in my opinion are Hacker Malicious and Vigilante Hacker

About hackers(hackers in black hat)

These are cybercriminals, mostly using hacking for their monetary gain.

They look for flaws in people's computers, organizations or banking systems and use those vulnerabilities to gain access to networks and steal private information.

They can then use various scams to trick you into giving them money or even gain direct access to your bank account.

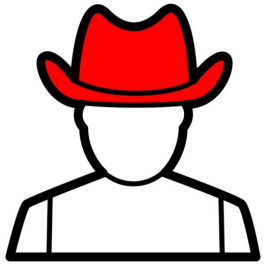


About hackers in red hat

Red hat hackers are similar to white hat hackers, but there is a big difference in their work.

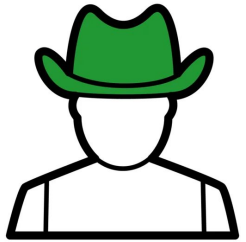
That hackers are the vigilantes of the hacker world.

They don't play by the rules, they fight back. Red hat hackers launch full-scale attacks against cybercriminals, using a range of aggressive methods to eliminate the threats of black hat hackers.



Green hat hackers

These are beginners who want to become professional hackers. They have a great desire to learn and get new hacking skills. You can often find them on forums dedicated to hacking.

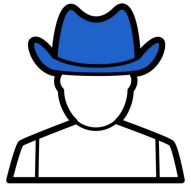


Blue Hat Hackers

They are amateur hackers, not interested in learning the intricacies of hacking.

Their only goal is to get back at someone.

They are not as dangerous as the black hat, but if they want revenge, they will use all their strength to get their adversary back.



About Spam

Spamming is the use of messaging systems to send multiple unsolicited messages (**spam**) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, for any prohibited purpose (especially the fraudulent purpose of phishing), or simply sending the same message over and over to the same user.

While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social spam, spam mobile apps,television advertising and file sharing spam.

It is named after Spam, a luncheon meat, by way of a Monty Python sketch about a restaurant that has Spam in almost every dish in which vikings annoyingly sing "Spam" repeatedly.

Phishing what is this?

- **Phishing** is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.
- Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim.
- As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.
- Phishing in Avito is very popular in Russia at the moment. Under the guise of a seller, people send in a link and use it to transfer money and the buyer does not receive the goods.
- Such people are called scammers in their world of cyber criminals

Phishing in Email

Most phishing messages are delivered by email, and are not personalized or targeted to a specific individual or company–this is termed "bulk" phishing. The content of a bulk phishing message varies widely depending on the goal of the attacker–common targets for impersonation include banks and financial services, email and cloud productivity providers, and streaming services. Attackers may use the credentials obtained to directly steal money from a victim, although compromised accounts are often used instead as a jumping-off point to perform other attacks, such as the theft of proprietary information, the installation of malware, or the spear phishing of other people within the target's organization. Compromised streaming service accounts are usually sold directly to consumers on darknet markets.

Threat identies

A threat to information security is understood as a set of conditions and factors, the implementation of which leads to a situation in which the organization's information security is in the risk zone.

The result of the implementation of risk is an event, the occurrence of which has economic or other adverse consequences for a person, organization or state.

The format of the information damage can be threefold - leakage, change or violation of the level of availability. But the consequences can range from man-made accidents to loss of funds from card accounts or disclosure of compromising information.

Threats information

In the process of analyzing threats to information it is necessary to evaluate:

- the source of risk;
- risk area;
- the hypothetical perpetrator;
- the probability of the risk's realization;
- the degree of damage from its realization;
- the ratio of the costs necessary to minimize the risk, and the loss caused in case of its realization.

Conclusion on information security.

The conclusion is that there are a lot of hackers in the world, but there are also white hackers who eliminate dark hackers.

The world is evolving, and so are hackers. Many technologies are being developed every day to remove all hackers from the world.

Therefore, use anti-virus and do not go to strange links, do not download unknown files, or suddenly you run a etherium miner on your computer and you will be helped only by reinstalling windows.

Presentation test.

What are the most dangerous hackers?

- Black hackers (1)
- Blue hat hackers
- Green hat hackers
- Red hat hackers

What is this phishing?

- Is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker (1)
- Mass mailing of advertising correspondence to people who have not expressed a desire to receive it. Spammers are called spammers.
- A form of social provocation or bullying in online communication, used both by personified participants interested in greater recognition, publicity, and epatage, as well as by anonymous users without the possibility of their identification.
- Non-thematic messages in Internet forums and chats, often occupying large volumes

Put the information in the right order

- the source of risk.(1)
- risk area.(2)
- the hypothetical perpetrator.(3)
- the probability of the risk's realization.(4)
- the ratio of the costs necessary to minimize the risk, and the loss caused in case of its realization.(6)
- the degree of damage from its realization.(5)

What types of phishing do you know?

Tell us about phishing on the Internet that you know of to date. Have you received spam or phishing emails?

Would you like to be a white hacker who eliminates cybercrime. Or on the contrary want to become dark, describe why you would like to become one of them?