



1. What consequences of malicious software infections do you know/experienced? Give two situations:

The most common answers given by the student in this question were all connected to the idea of data security.

data stealingmining

Data theft

System Damage

data lossloss

malware

data or lose

Data loss

data leakage haven't experienced

Trojan horse software infections easily steal

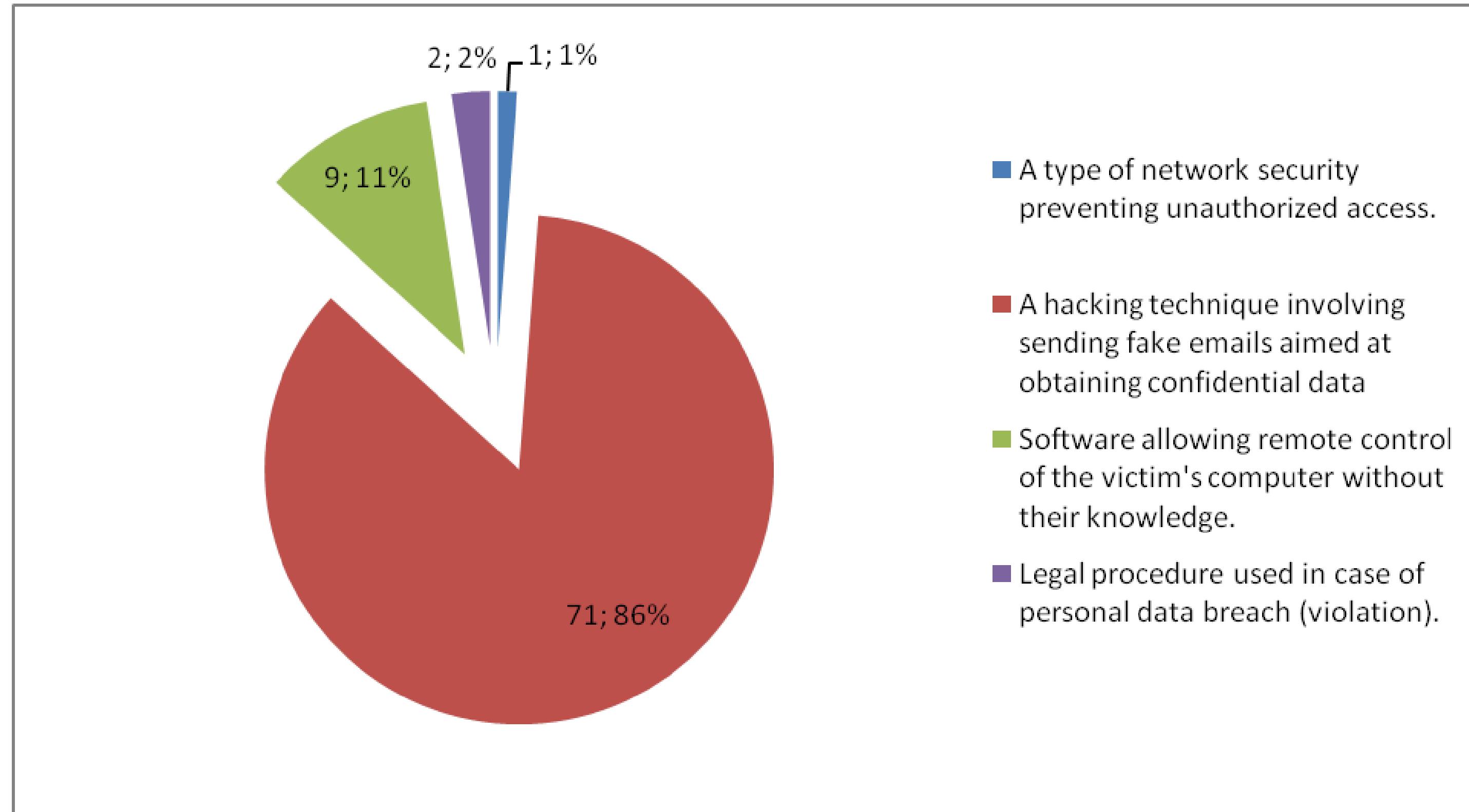
data

Information personal informations

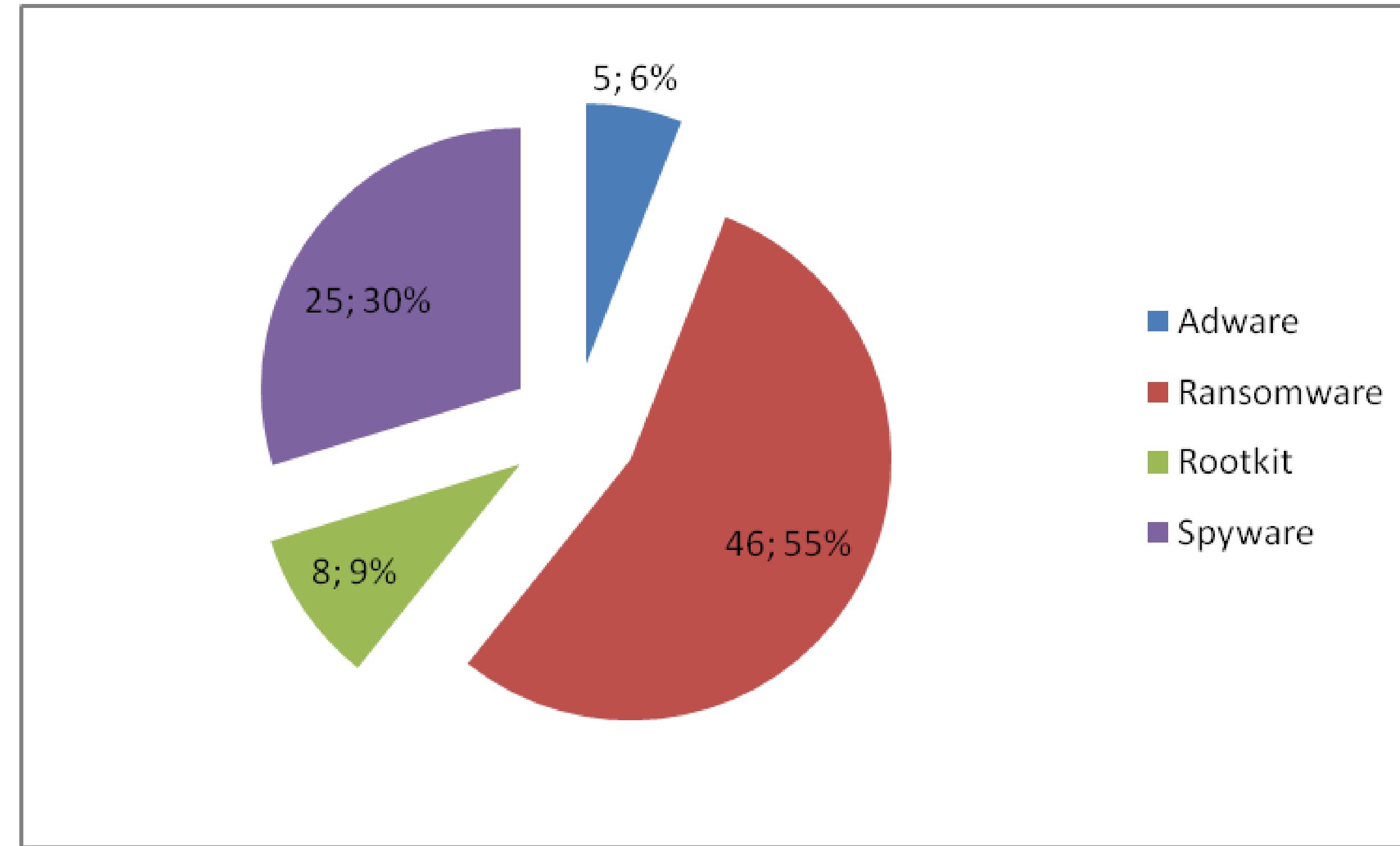
device computer Financial Loss

personal data Data Breach

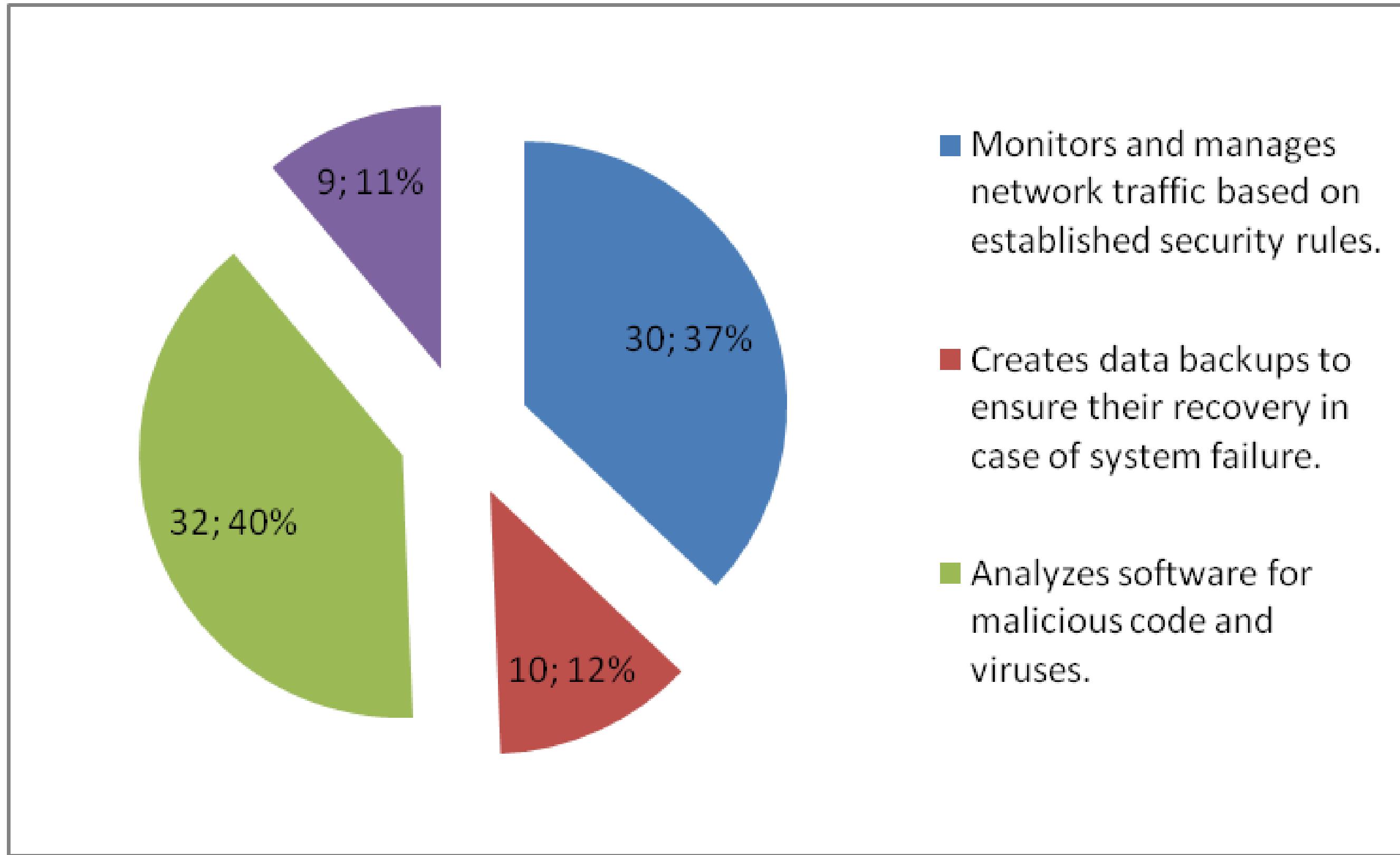
2. What is "phishing"?



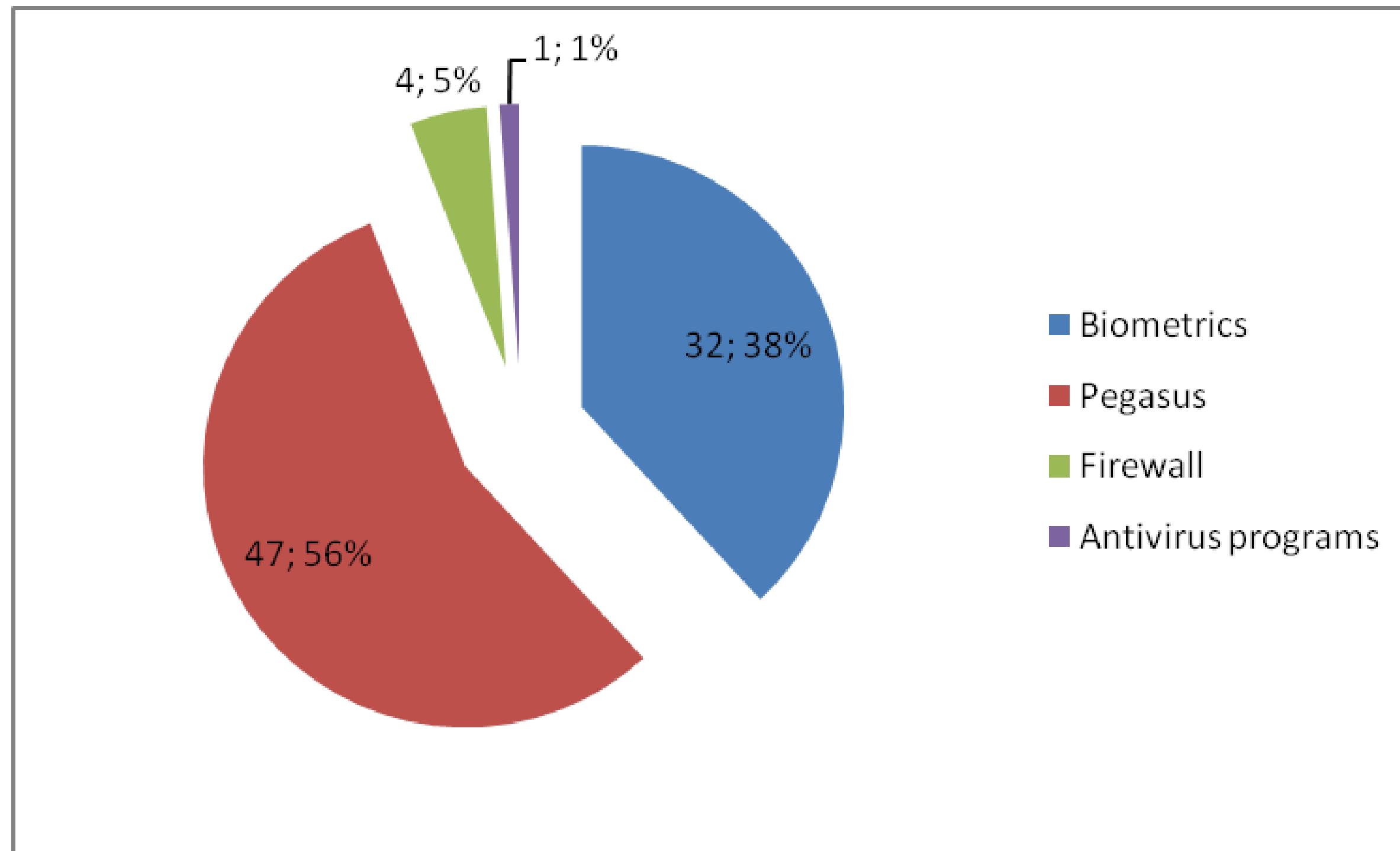
3. What type of malware encrypts user files after infecting the system, demanding ransom for their release?



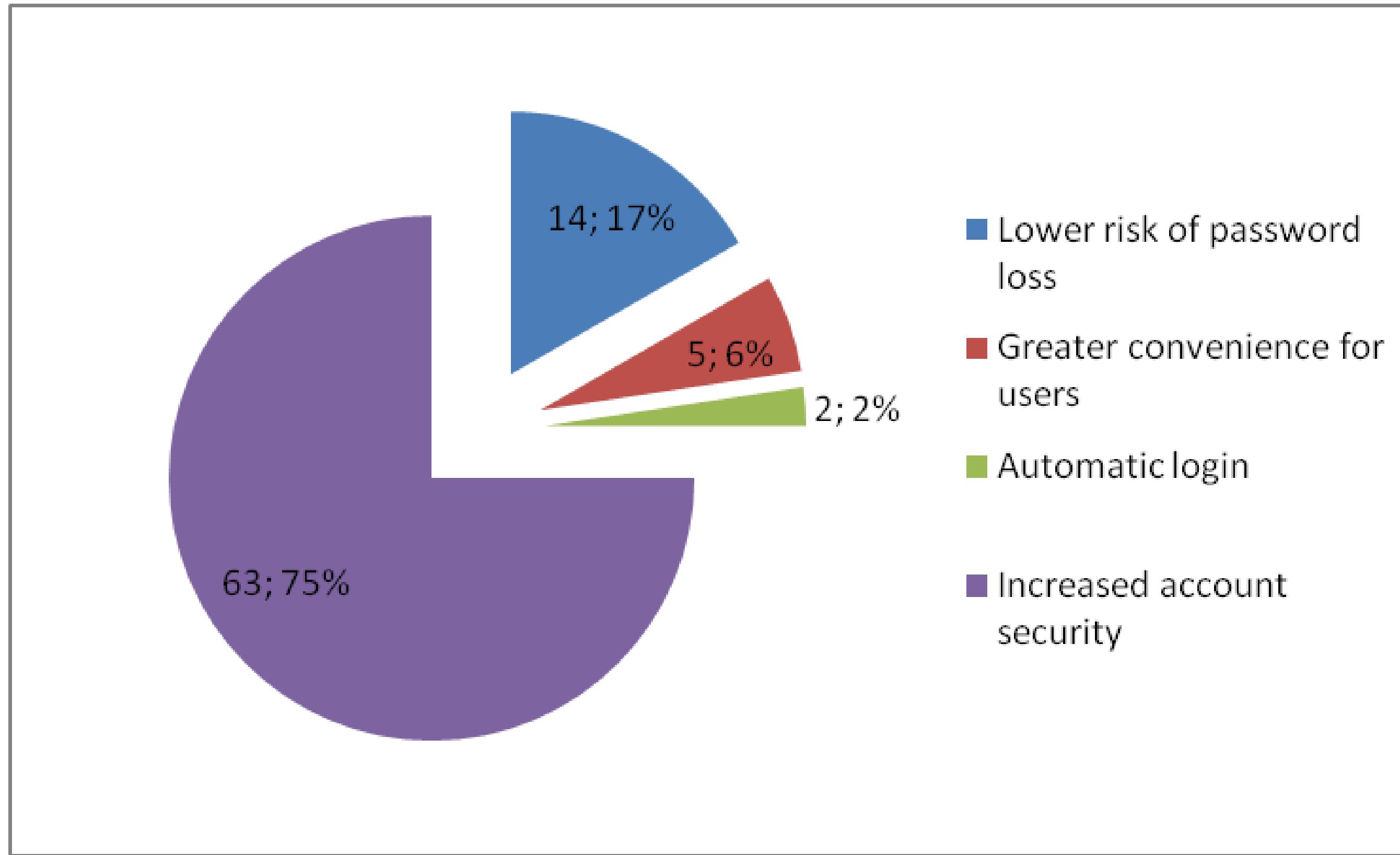
4. What role does a firewall play in computer network security?



5. Which of the following is NOT a type of computer security (protection)?



6. What are the benefits of using two-factor authentication?



7. What should you do to secure your account when using online services?

Give 3 such actions:

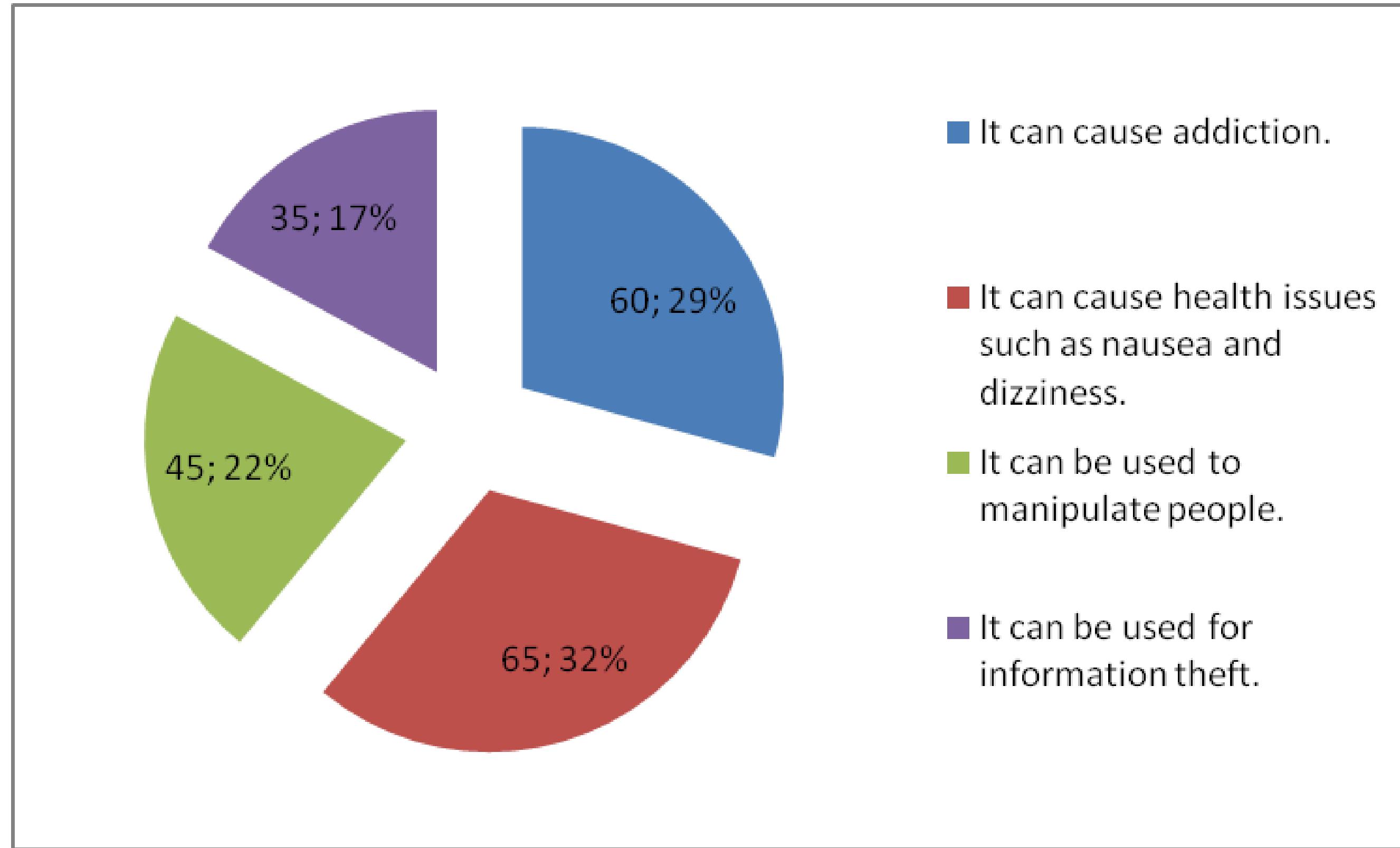
The answers to this question varied, however, the biggest group mentioned password as the key to online safety.

strong password

use
share
account
hard password
better password
update your software
passwords for different
simple passwords

factor authentication
double factor personal information
complicated passwords
factor verification
youir passwords
different passwords
password is okej
good password
factor authentication2
passwords on each website

8. What threats are associated with virtual reality? (multiple choice question)



9. What is the potential usage of virtual reality technology in education?

List 2 such examples:

The answers to this question were as follows:

students can do experiments

immerse students events places

Education

history fun for students

virtual reality better students VR

new

field trips

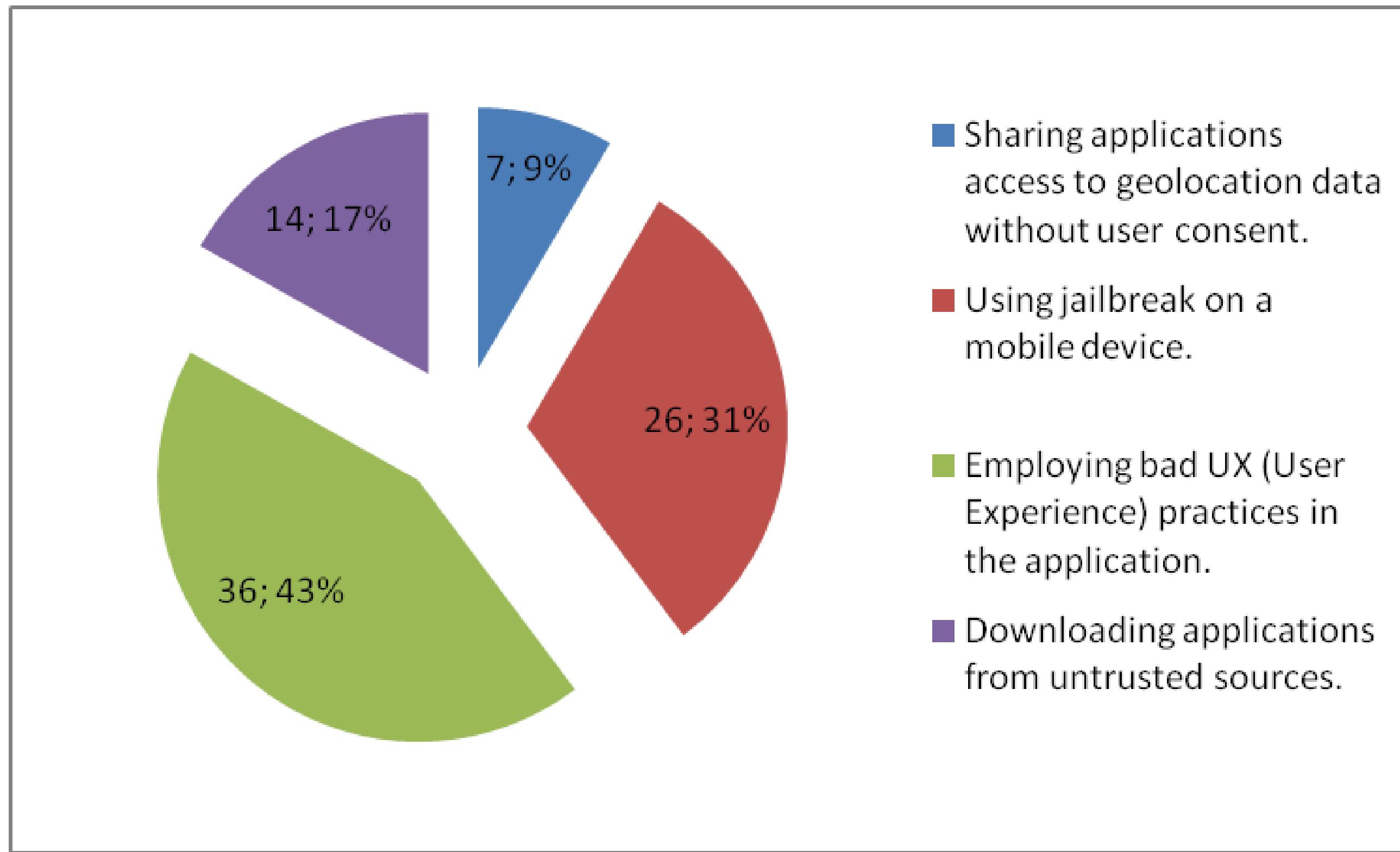
lab environments geography informations

medicine virtual field

virtual environments

things easier

10. Which of the following phenomena is not a threat to user security in the context of mobile applications?

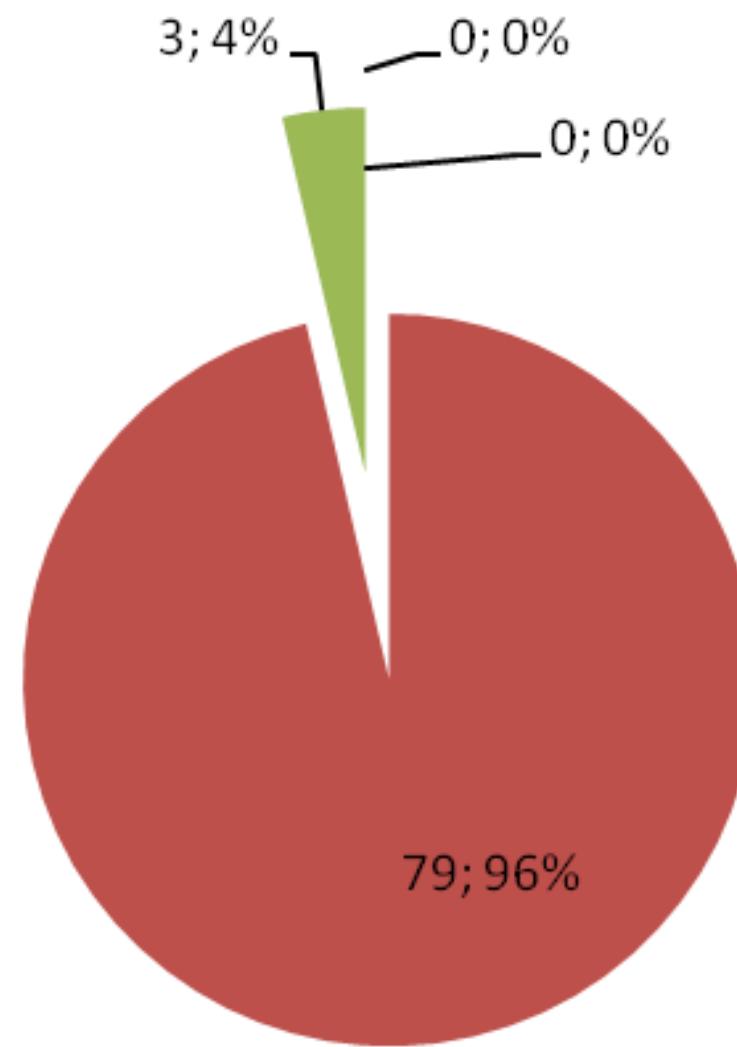


11. List 3 potential threats associated with sharing access to user geolocation data within applications:

The answers to this question were as follows:

location information
personal data surveillance Steal information threats unwanted contact
Privacy breach misused data Location location data
user data physical safety IP address Security Risks private data
Data Breaches data and documents don't know financial data

12. What is a "fake online store"?



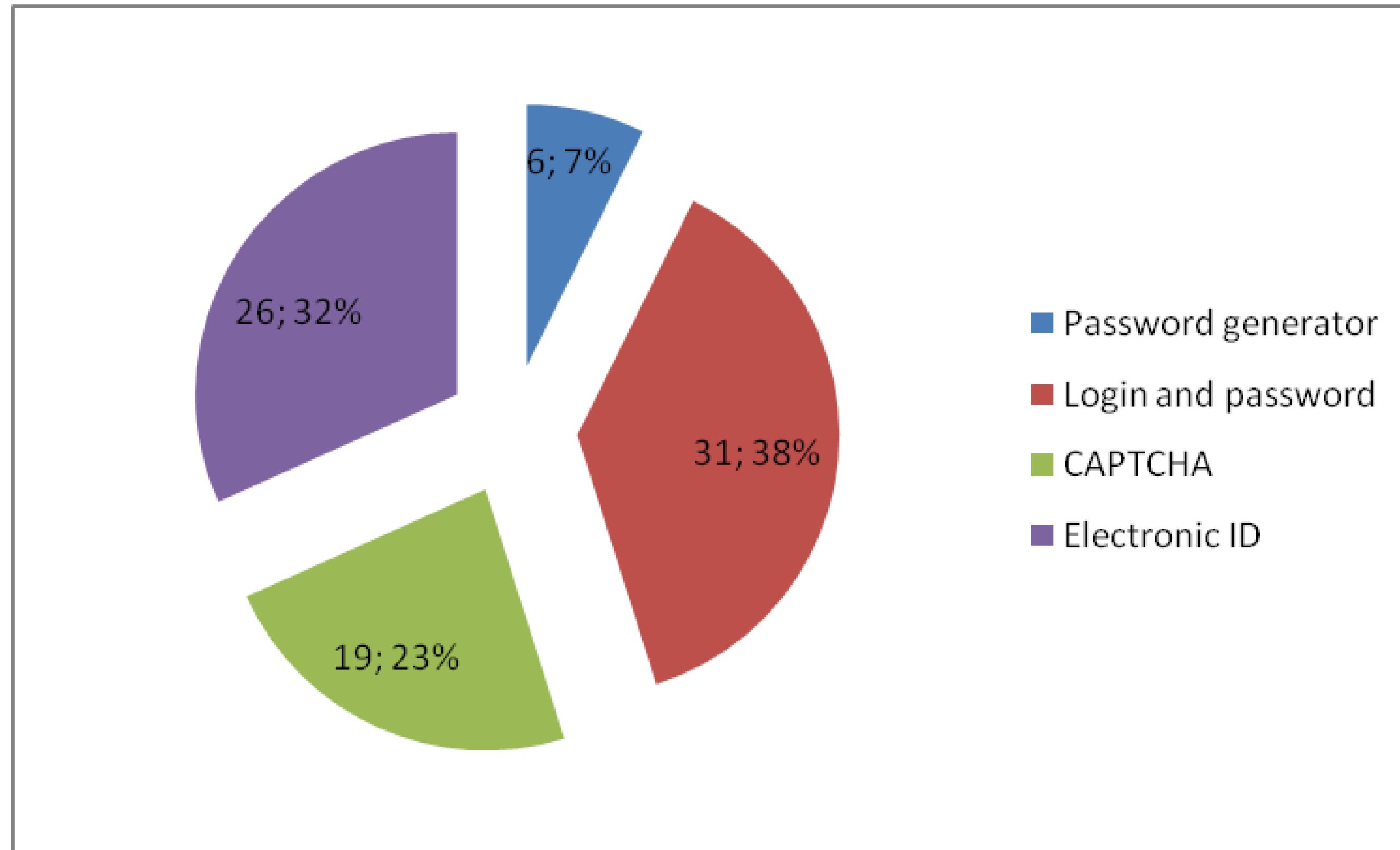
- An online store with a high reputation and many positive reviews.
- A website pretending to be a real store, deceiving customers and stealing their data or money.
- A store that sells counterfeit popular products.
- An online store offering only products from legal sources.

13. What methods can hackers use to try to take control of a user's account during purchases? Provide two methods:

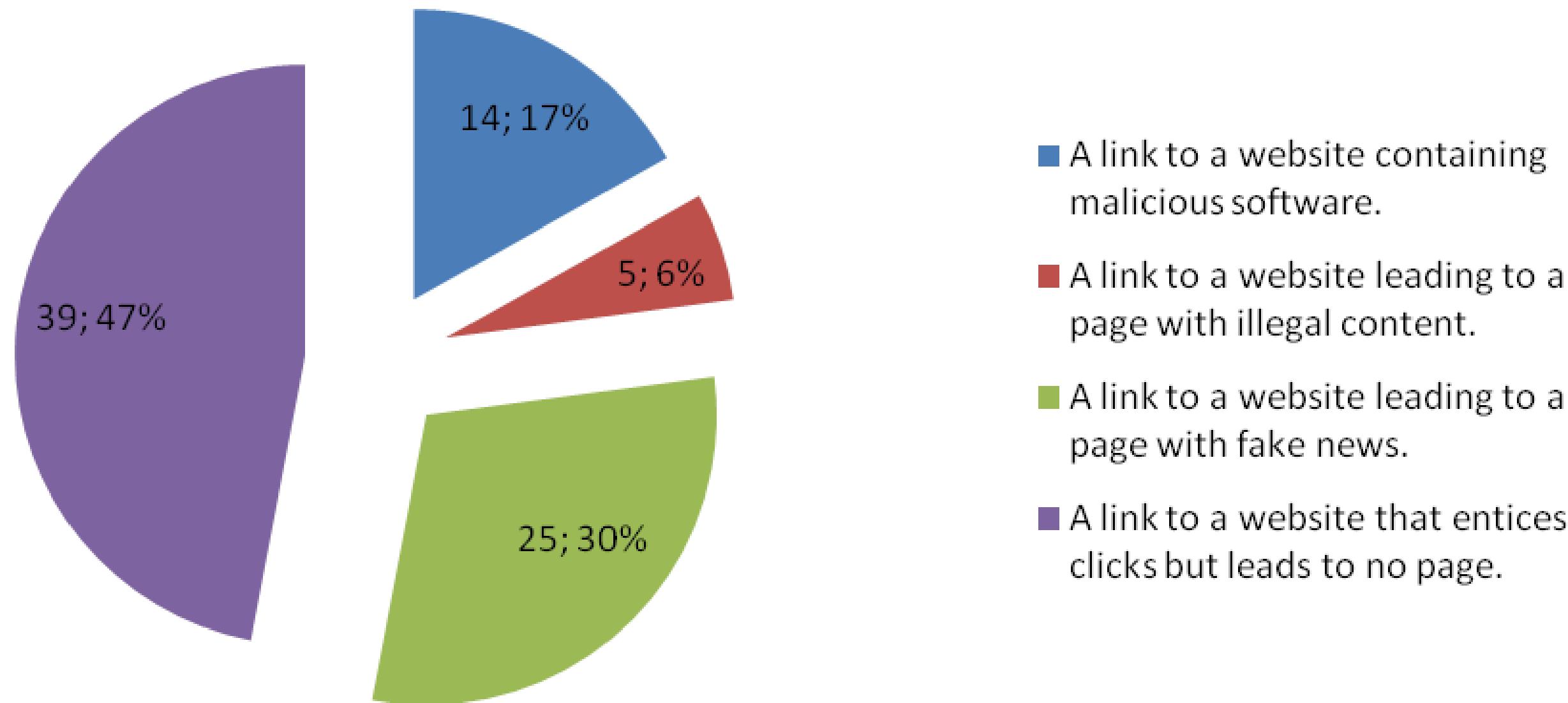
The answers to this question were as follows:

fake item data breaches
fake sites Credential
Credential Cracking user card
Credential stuffing
fake email
fake
fake website
Phishing and Clickjacking
spyware login credentials
account Force Credential
information malicious code

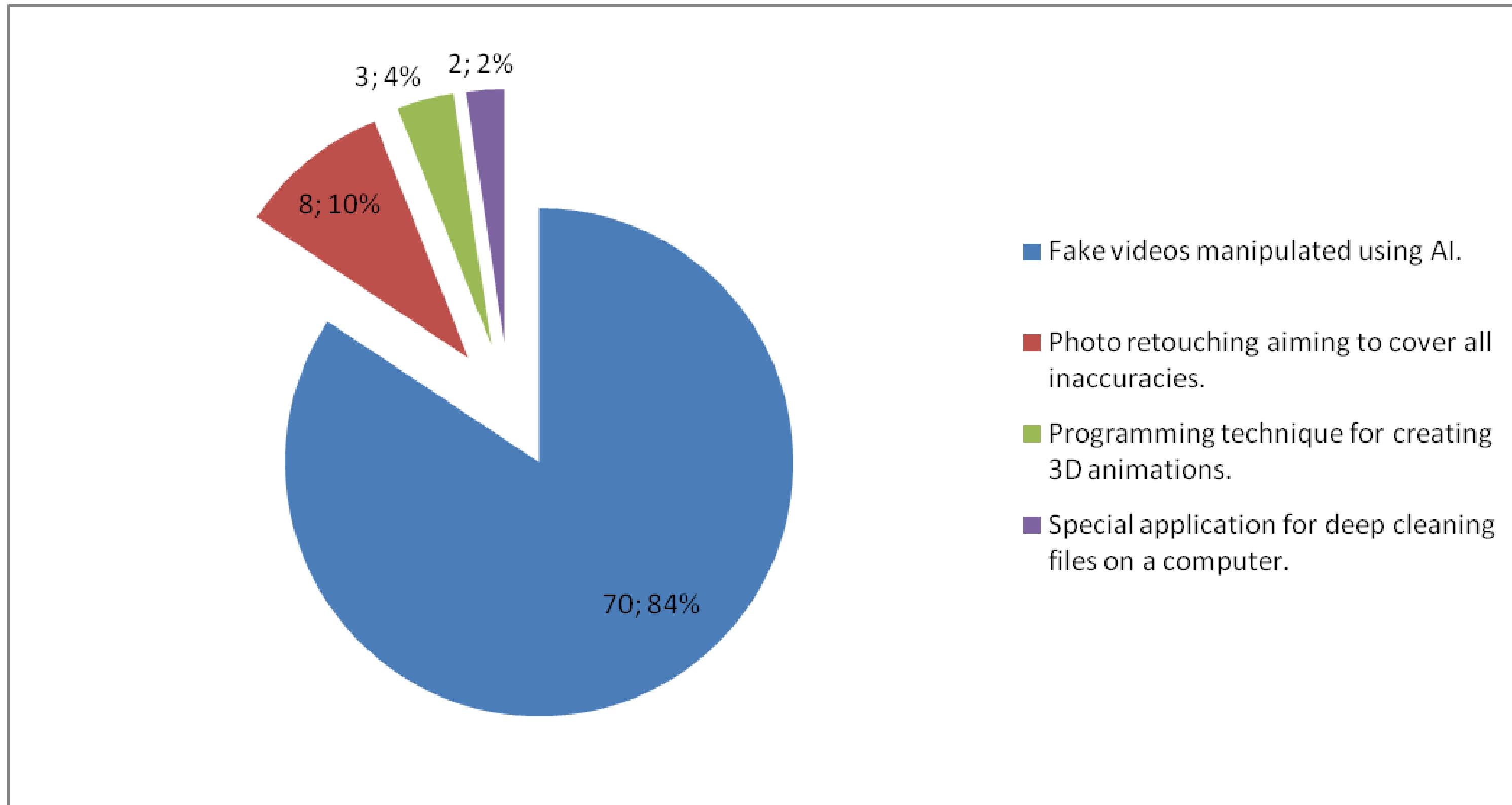
14. Which of the following are examples of authentication methods during online purchases?



15. What is clickbait?



16. What is deepfake?



17. What are the possible consequences of oversharing, i.e., excessive sharing of personal information on social media? List 2 such consequences:

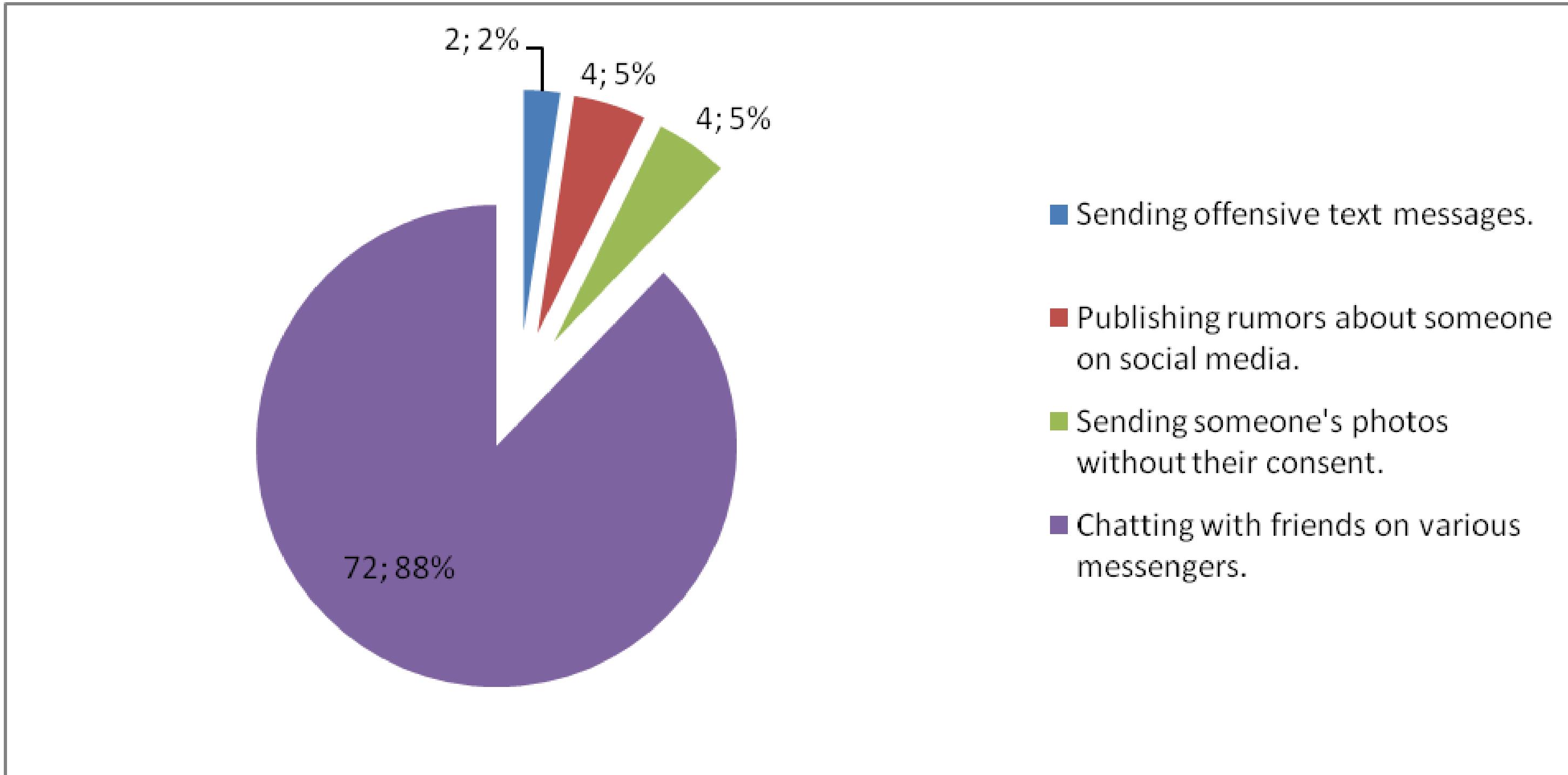
The answers to this question were as follows:

personal data
image theft
zneužití osobních
use
informations against the person
stalking and kidnaping

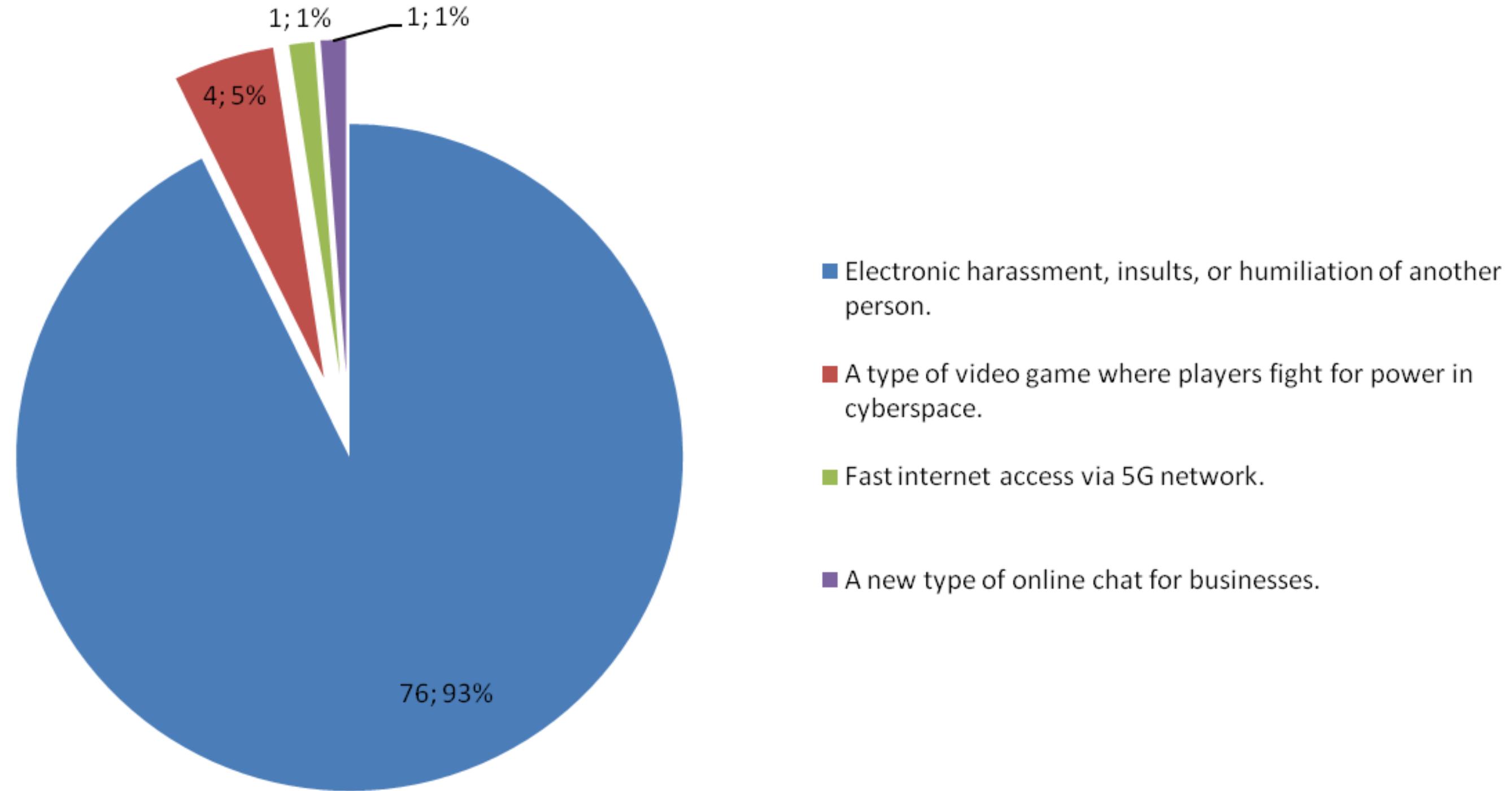
false information
theft and fraud
money
identity theft
share
data theft
Privacy violations

people
Privacy
osobních údajů
personal info
privacy breaches

18. Which actions are NOT considered cyberbullying?



19. What is "cyberbullying"?



20. What is "media multitasking"?

