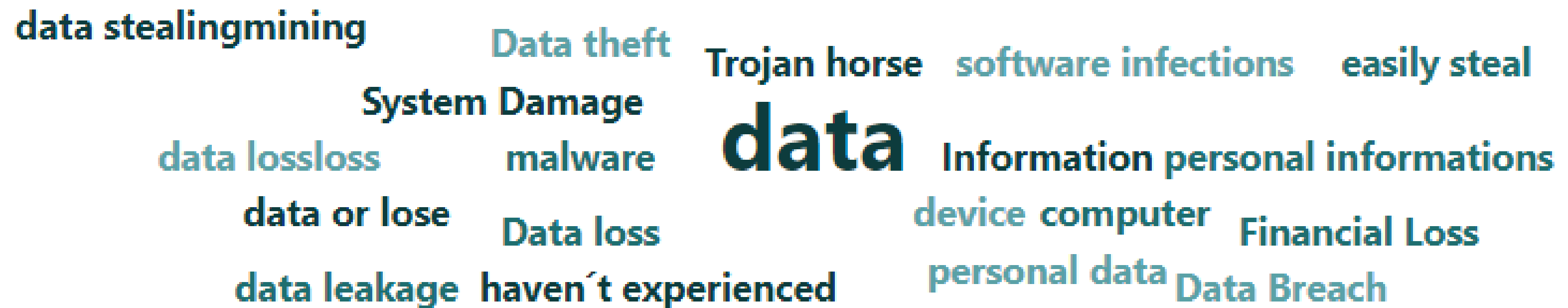




1. What consequences of malicious software infections do you know/experienced? Give two situations:

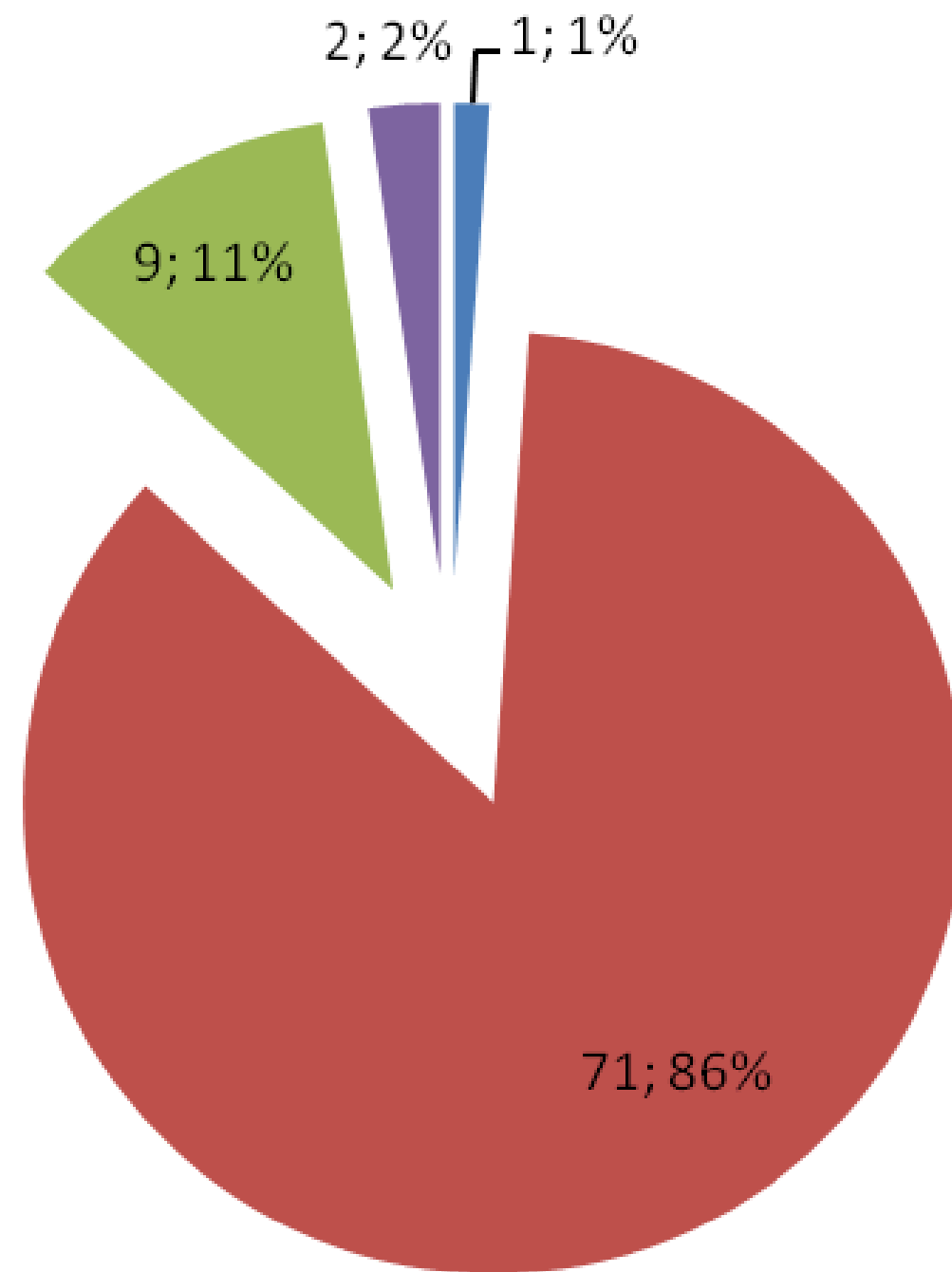
The most common answers given by the student in this question were all connected to the idea of data security.



A word cloud of terms related to data security and malicious software infections. The word 'data' is the largest and most central. Other prominent words include 'Trojan horse', 'software infections', 'easily steal', 'Information personal informations', 'Financial Loss', 'Data Breach', 'personal data', 'device computer', 'Data loss', 'malware', 'System Damage', 'Data theft', 'data stealing', 'data loss', 'data or lose', 'data leakage', and 'haven't experienced'.

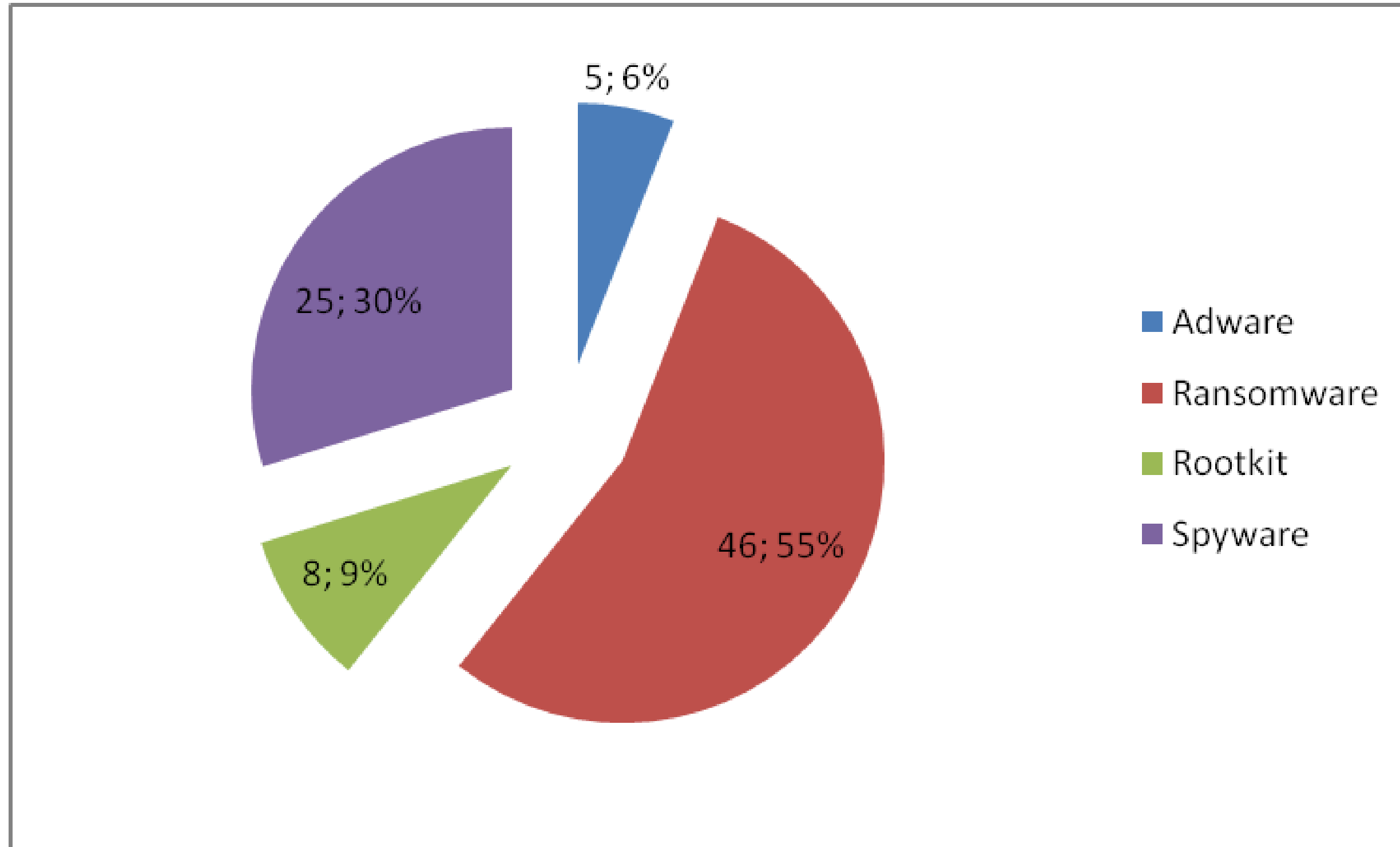
data stealing mining Data theft Trojan horse software infections easily steal
System Damage data loss loss malware data data or lose Data loss Information personal informations
device computer Financial Loss
data leakage haven't experienced personal data Data Breach

2. What is "phishing"?

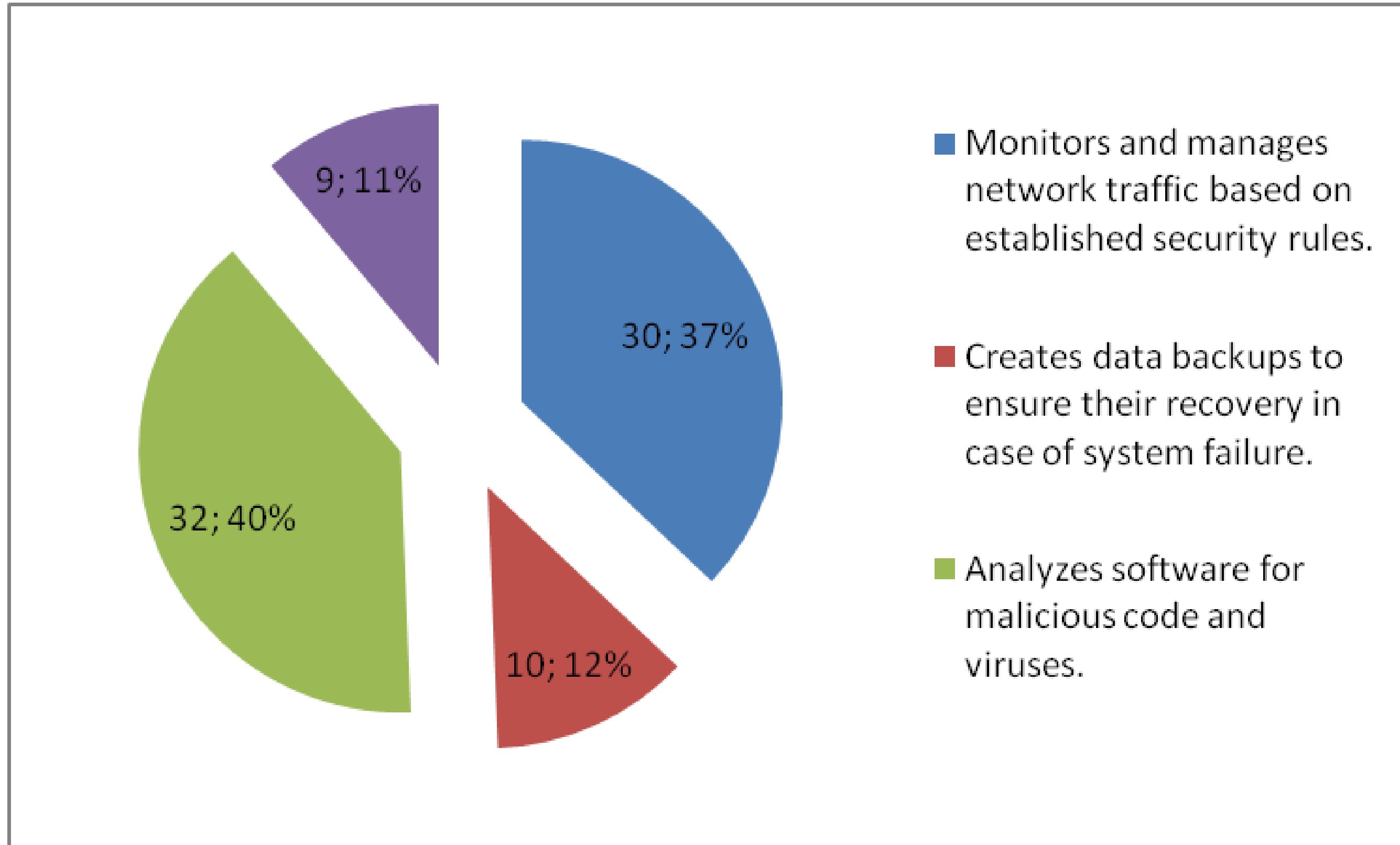


- A type of network security preventing unauthorized access.
- A hacking technique involving sending fake emails aimed at obtaining confidential data
- Software allowing remote control of the victim's computer without their knowledge.
- Legal procedure used in case of personal data breach (violation).

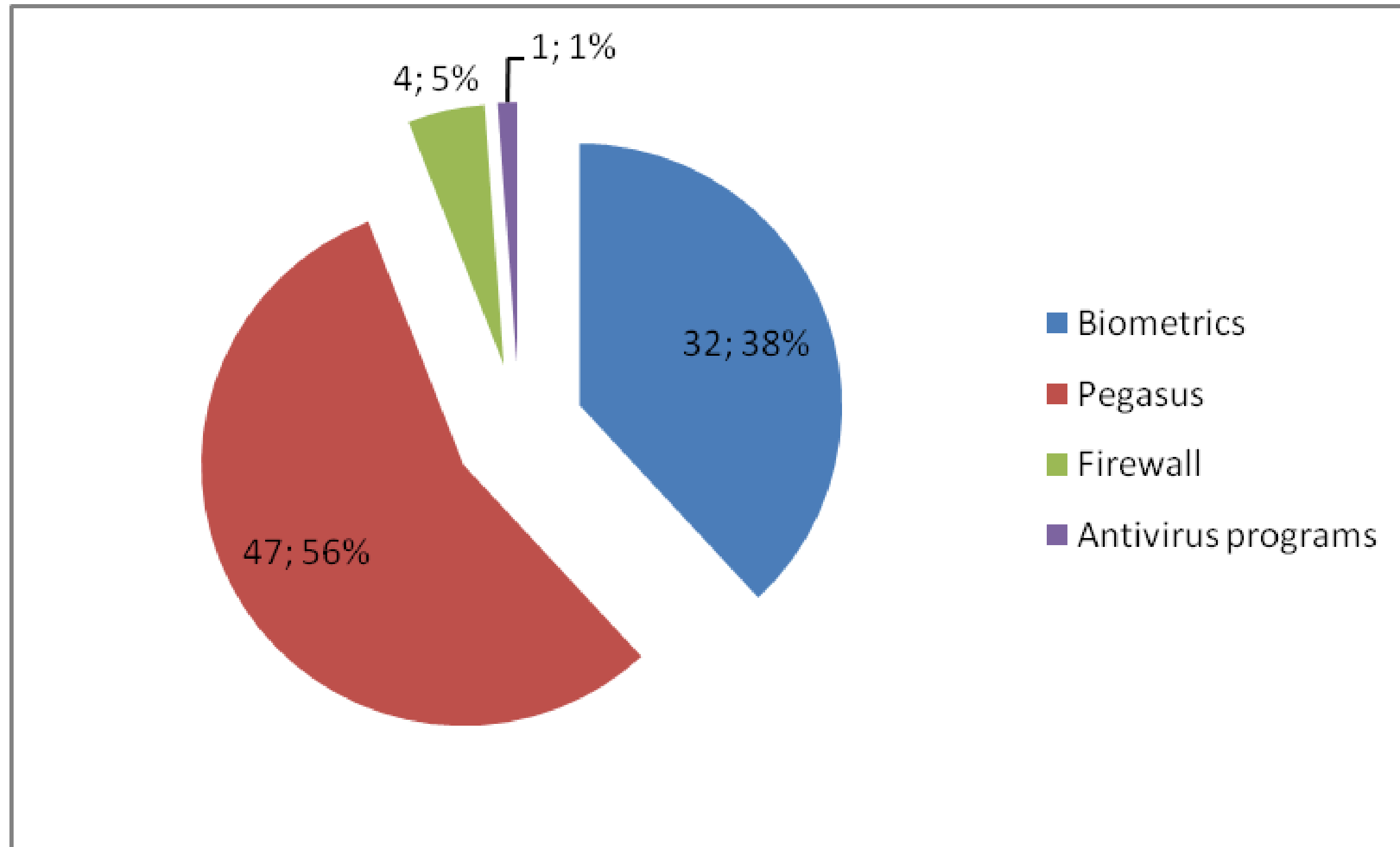
3. What type of malware encrypts user files after infecting the system, demanding ransom for their release?



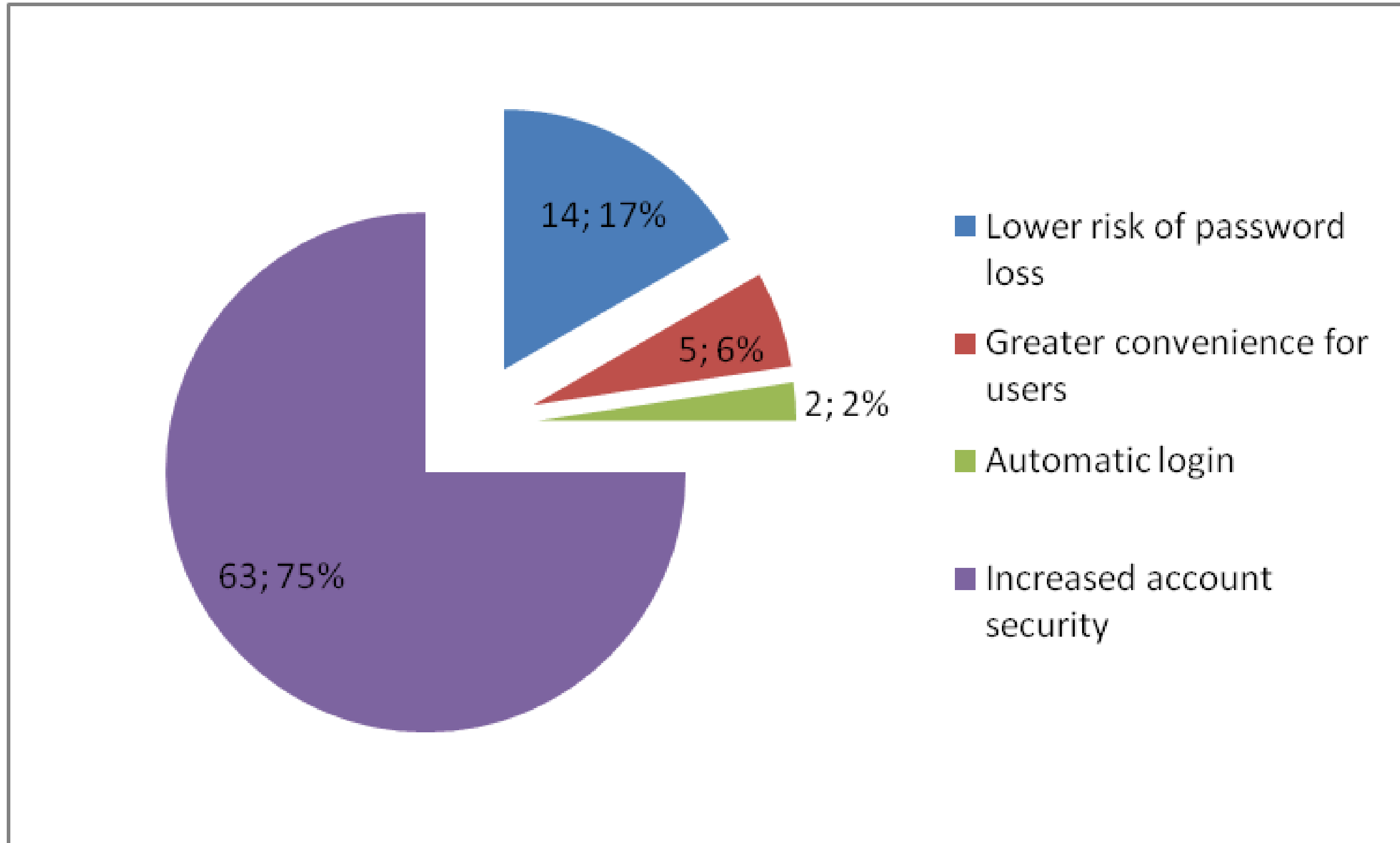
4. What role does a firewall play in computer network security?



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:

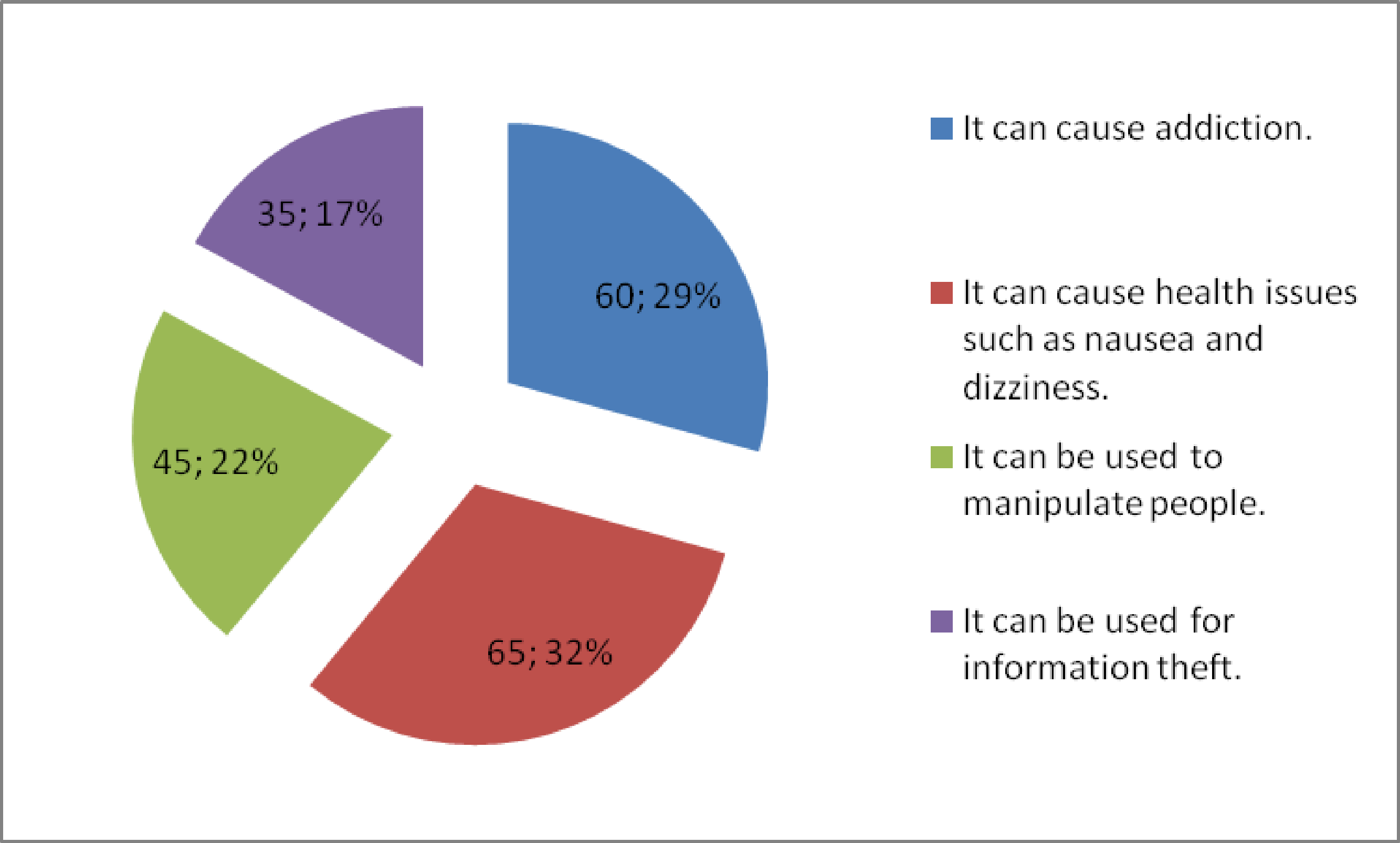
The answers to this question varied, however, the biggest group mentioned password as the key to online safety.



A word cloud of security-related terms. The words are arranged in a circular pattern, with 'strong password' being the largest and most prominent. Other large words include 'factor authentication', 'use', and 'passwords on each website'. Smaller words include 'good password', 'password is okej', 'different passwords', 'your passwords', 'double factor personal information', 'factor verification', 'complicated passwords', 'share', 'account', 'hard password', 'better password', 'update your software', and 'simple passwords'.

password is okej good password passwords on each website
factor authentication2
your passwords different passwords
strong password
factor authentication use
double factor personal information share account hard password better password
factor verification complicated passwords update your software
passwords for different simple passwords

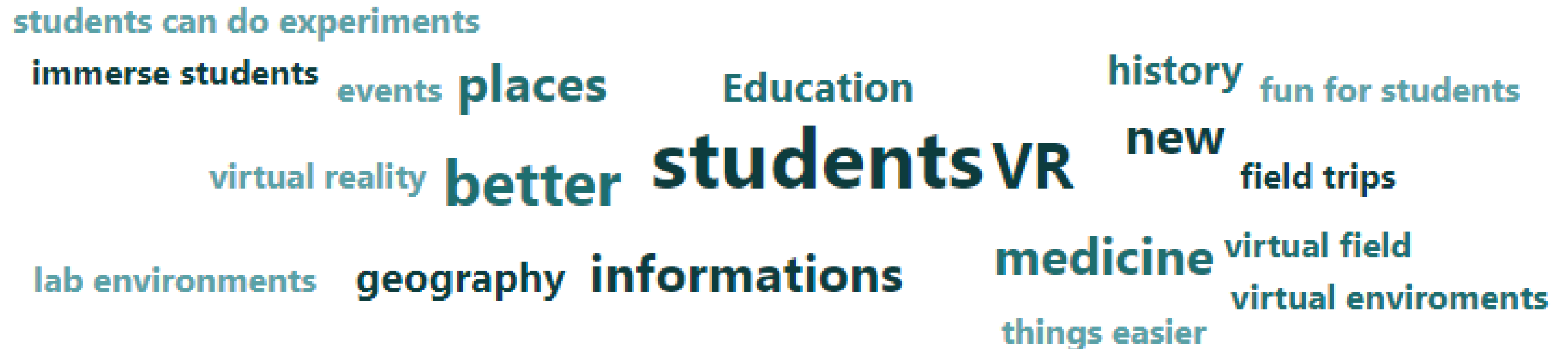
8. What threats are associated with virtual reality? (multiple choice question)



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

List 2 such examples:

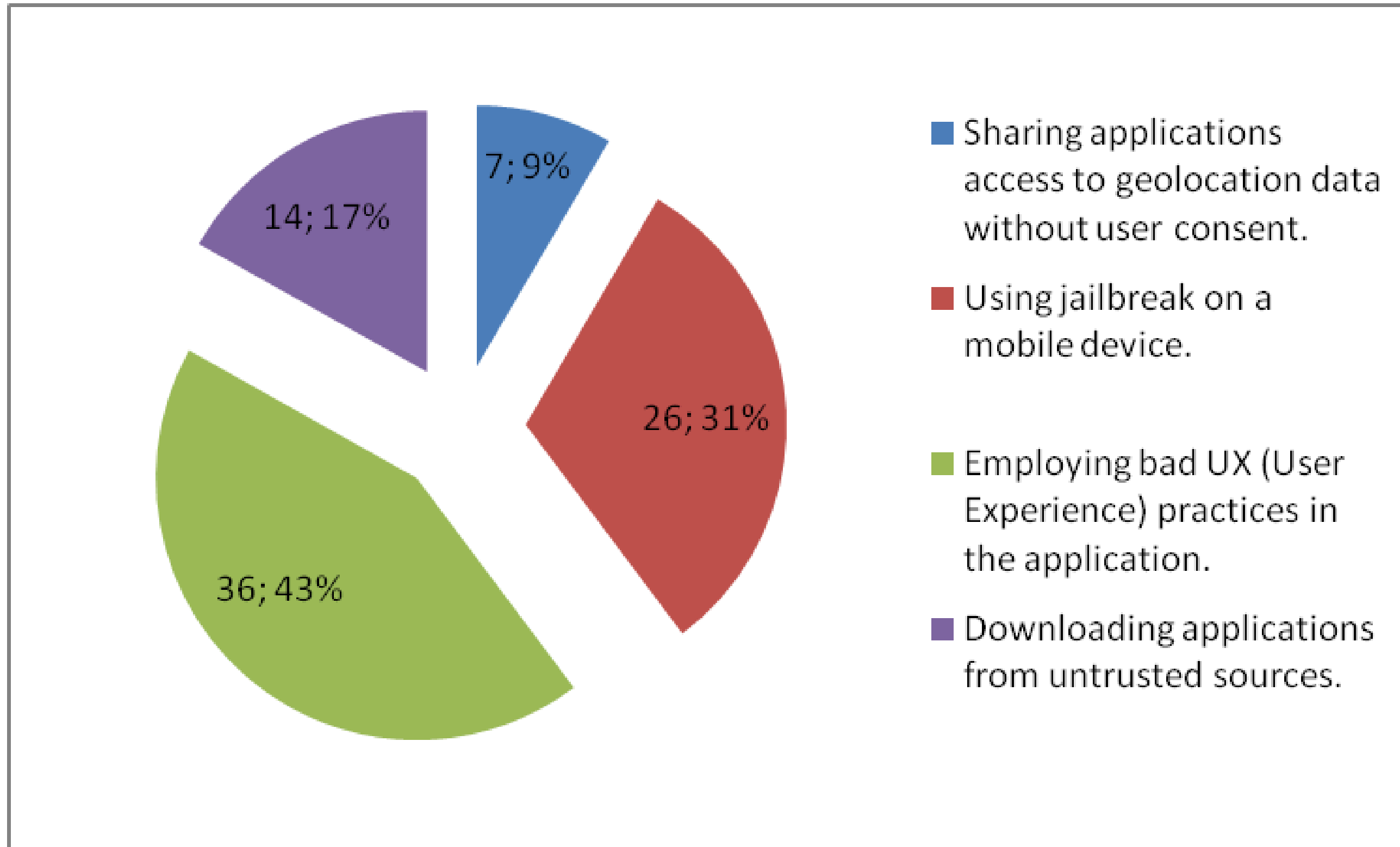
The answers to this question were as follows:



A word cloud of responses to the question 'What is the potential usage of virtual reality technology in education?'. The words are arranged in a circular pattern, with 'students' and 'VR' being the largest and most central. Other prominent words include 'better', 'information', 'medicine', 'places', 'Education', 'history', 'new', 'field trips', 'virtual reality', 'lab environments', 'geography', 'virtual field', 'virtual environments', 'things easier', 'fun for students', 'events', 'immerse students', and 'students can do experiments'.

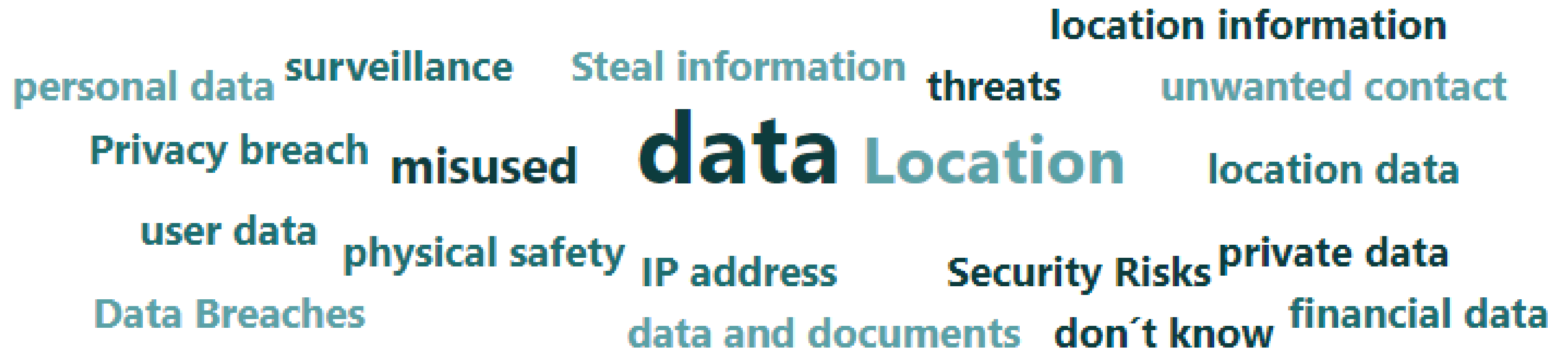
students can do experiments
immerse students events places Education history fun for students
virtual reality better students VR new field trips
lab environments geography information medicine virtual field
things easier virtual environments

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:

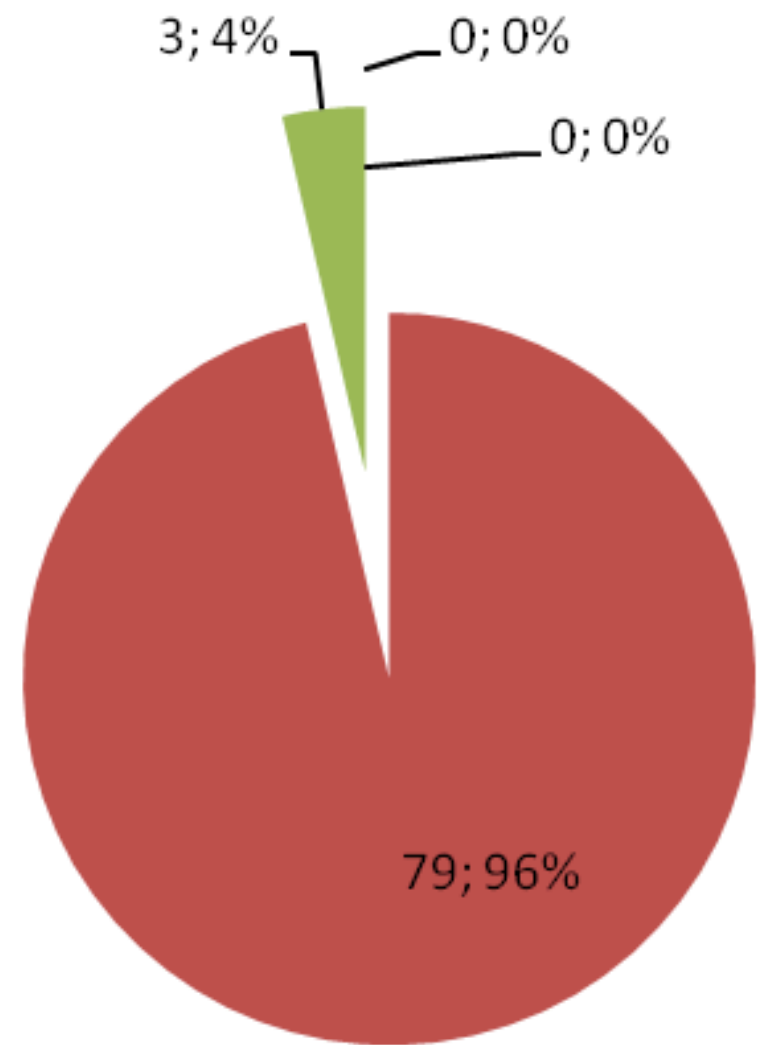
The answers to this question were as follows:



A word cloud of various threats and data types associated with sharing user geolocation data. The words are arranged in a non-uniform, overlapping manner, with some words being significantly larger than others. The colors of the words range from dark blue to light blue. The words include: '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', and 'financial data'.

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.

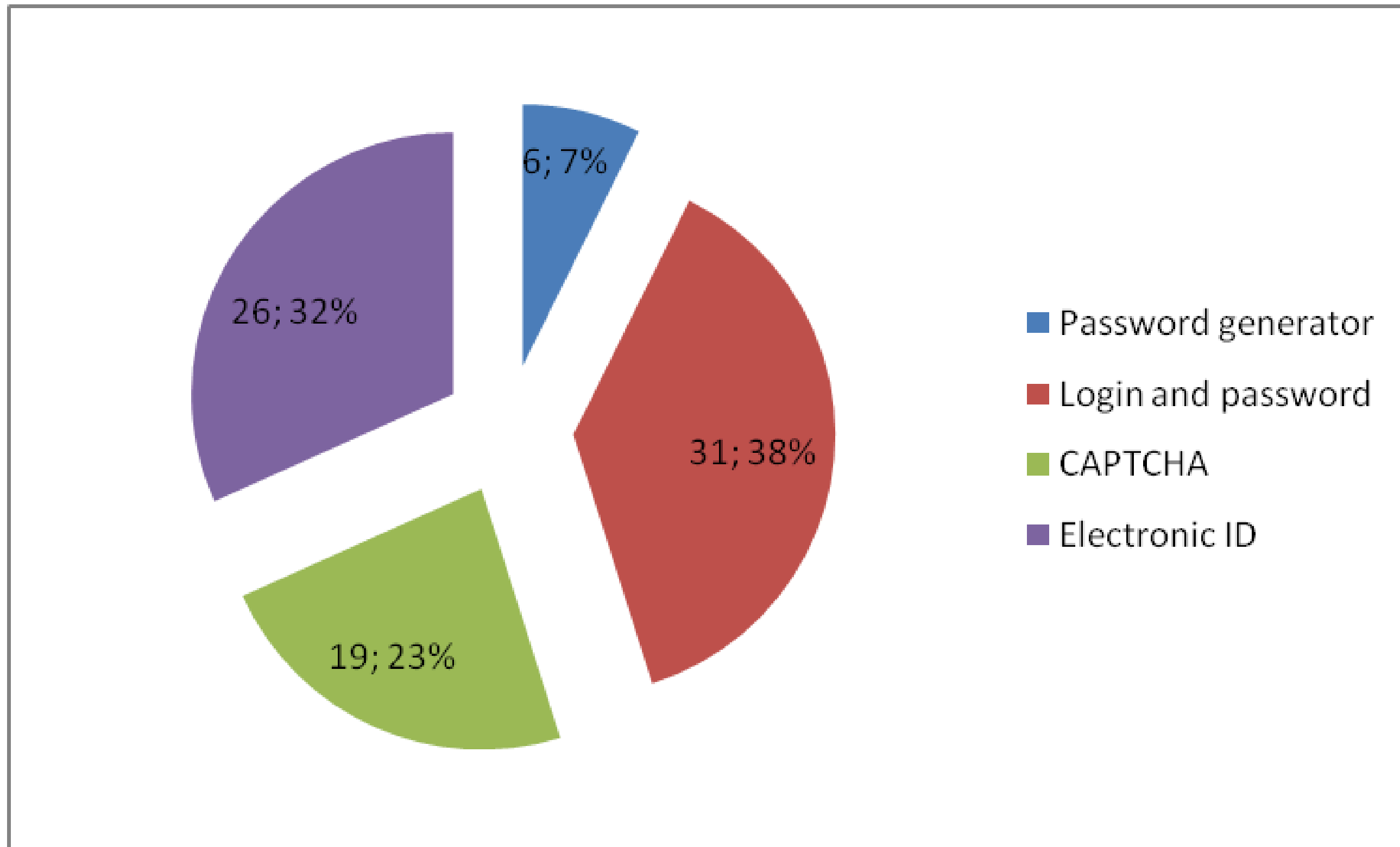
13. What methods can hackers use to try to take control of a user's account during purchases? Provide two methods:

The answers to this question were as follows:

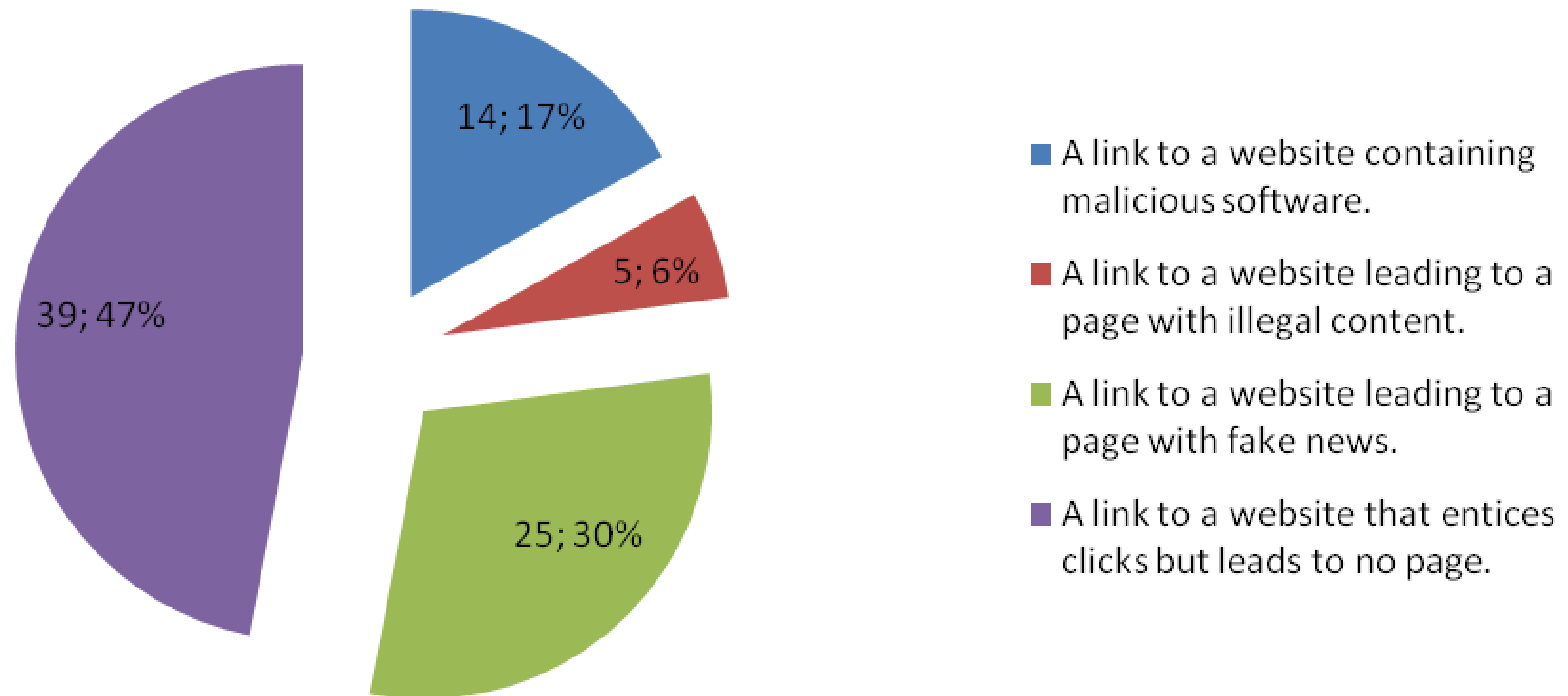
A word cloud of cybersecurity terms. The word 'fake' is the largest and most central. Other prominent words include 'Phishing and Clickjacking', 'Credential Cracking', 'fake email', 'login credentials', 'account', 'force credential', 'malicious code', 'information', 'fake website', 'card', 'user', 'Credential stuffing', 'fake sites', 'hackers', 'bank', 'data breaches', 'fake item', 'spyware', and 'login credentials'.

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

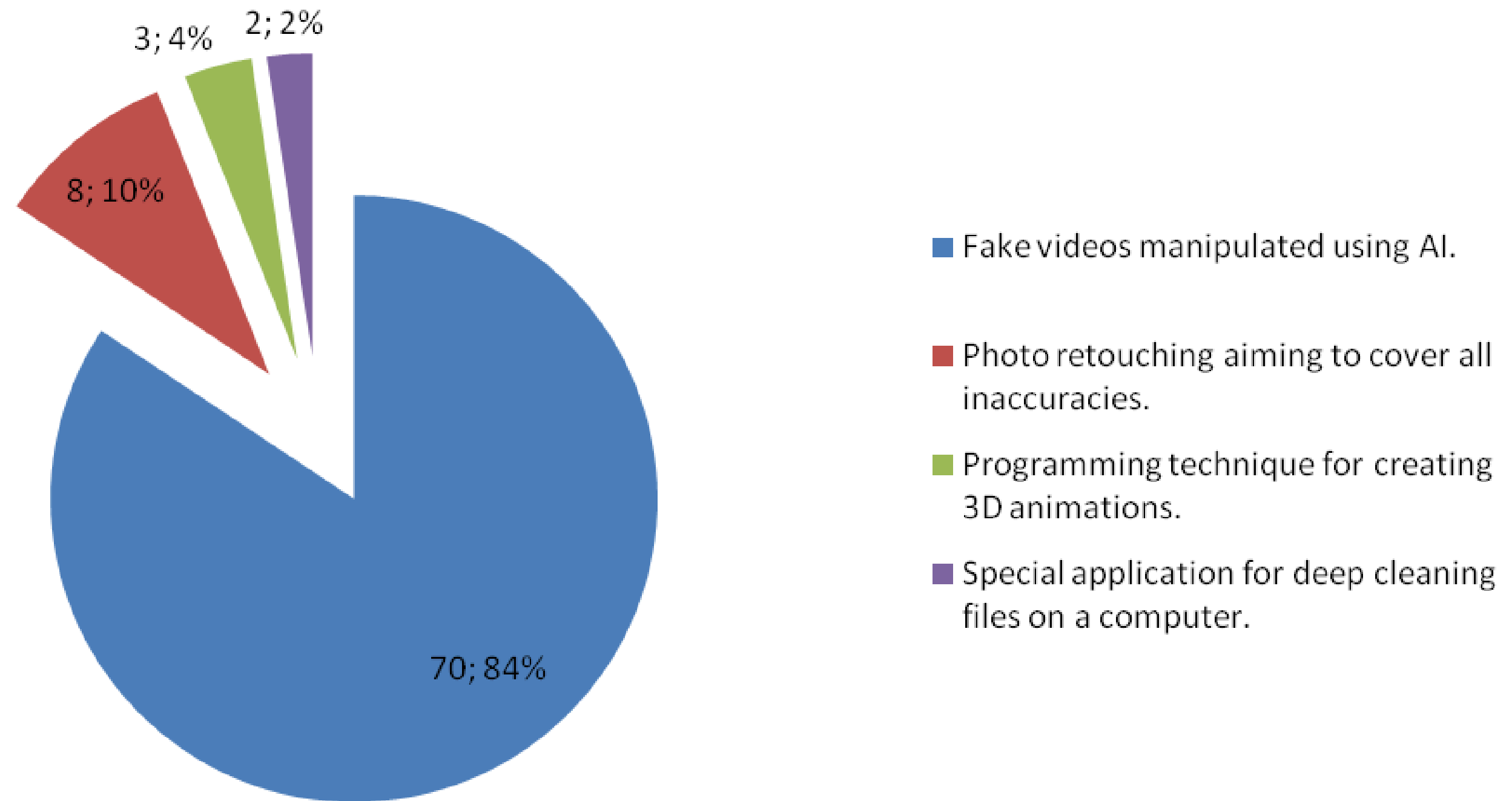
14. Which of the following are examples of authentication methods during online purchases?



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:

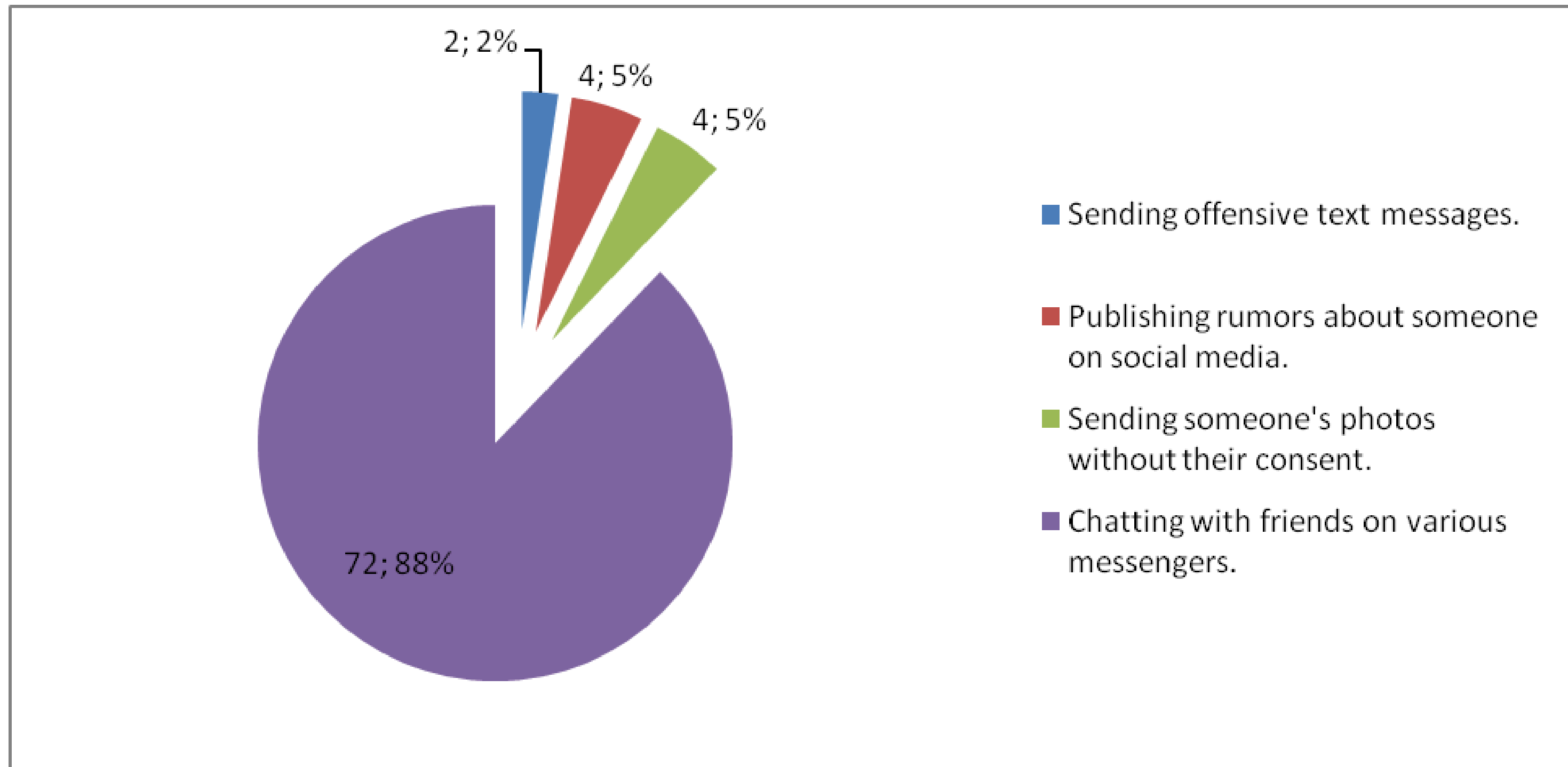
The answers to this question were as follows:



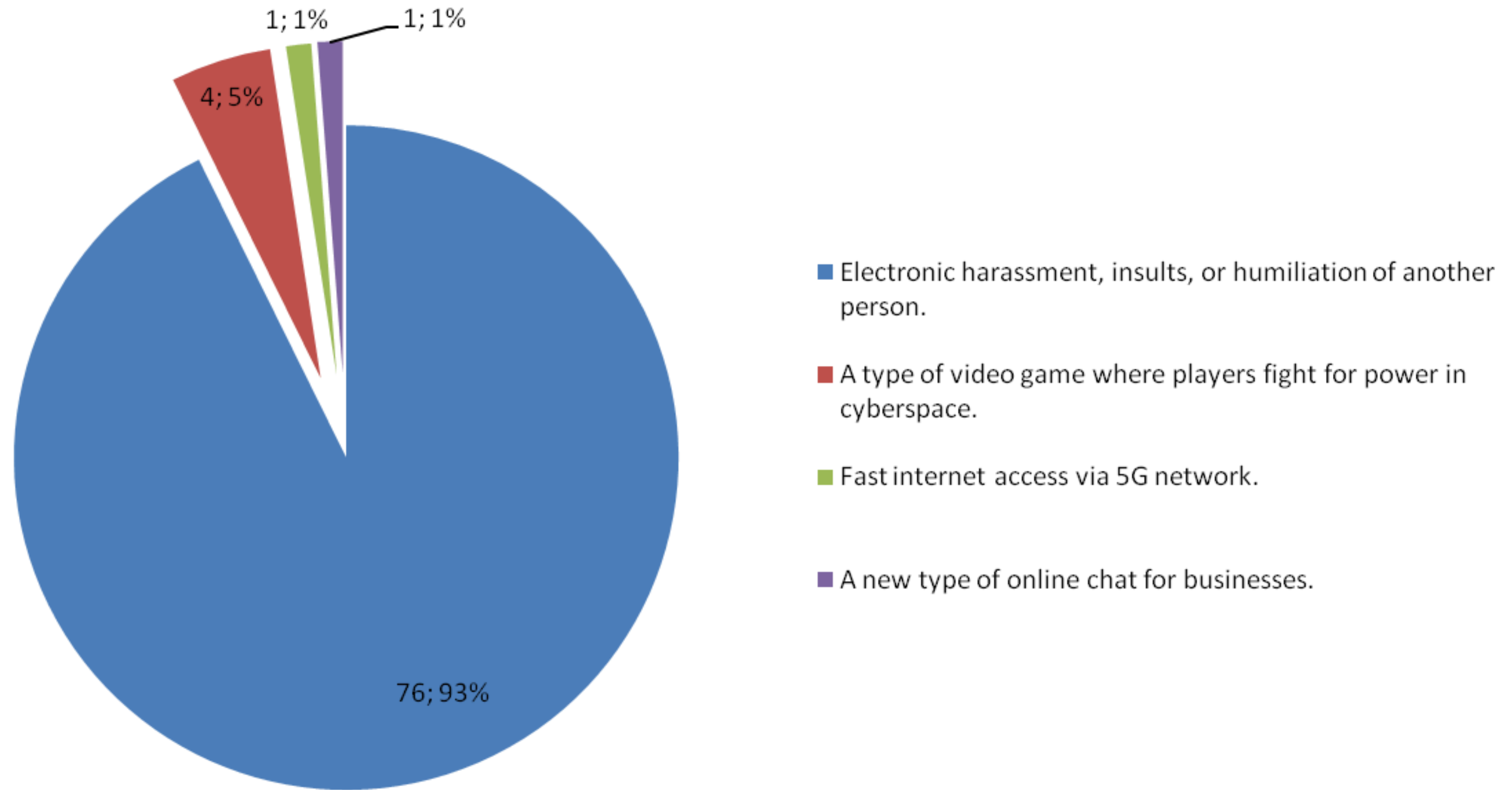
A word cloud illustrating the consequences of oversharing on social media. The words are arranged in a circular pattern around the central phrase "identity theft". The words are in various shades of blue and green, with some appearing in a lighter, semi-transparent font. The words include:

- personal data
- image theft
- zneužití osobních
- use
- information
- theft and fraud
- money
- redistribute information
- people
- personal info
- Privacy
- osobních údajů
- share
- data theft
- personal information
- Privacy violations
- privacy breaches
- informations against the person
- stalking and kidnaping

18. Which actions are NOT considered cyberbullying?



19. What is "cyberbullying"?



20. What is "media multitasking"?

