7.

1-T

2-F, all types

3-хз типо не пытается еще и обнаружить еси существует но а так T

4-T

5-F, look for a virus signature

6-F, unique

7-F, security experts

8-F,

1.

Espionage – шпионаж

Sabotage – саботаж

DOS – отказ в обслуживании

3.

a) Phishing - This tactic includes deceptive emails to steal information.

b) Spear Phishing - A spoofed email is used to carry out targeted attacks against individuals or businesses.

c) Baiting - It's an online and physical social engineering attack that promises the victim some gain.

d) Rogue Antivirus - Victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed.

e) Tailgating - It relies on human trust to give the criminal physical access to a secure building or area.

f) Pharming - It redirects website traffic to fraudulent websites that distribute malware, collect personal data, sell counterfeit products, and perpetrate other scams.

g) Shouldering (shoulder surfing) - It occurs when someone surreptitiously watches over your shoulder to nab valuable information.

h) Vishing - It is voice solicitation over the phone (voice+phishing).

Перевод:

a) Фишинг - Эта тактика включает в себя мошеннические электронные письма для кражи информации.

b) Спирфишинг - Используется поддельное электронное письмо для проведения целенаправленных атак на отдельных лиц или предприятия.

c) Подманивание - Это онлайн- и физическая атака социальной инженерии, обещающая жертве какую-то выгоду.

d) Разбойное антивирусное программное обеспечение - Жертвы вводятся в заблуждение, что на их компьютере установлен вредоносный код и что, если они заплатят, вредоносный код будет удален.

e) Хвостование - Она основана на доверии людей и позволяет преступнику физически проникнуть в безопасное здание или зону.

f) Фарминг - Он перенаправляет трафик веб-сайта на мошеннические веб-сайты, распространяющие вредоносное программное обеспечение, собирающие личные данные, продающие поддельные товары и совершающие другие мошеннические действия.

g) Шоулдеринг (шпионаж за плечом) - Это происходит, когда кто-то тайно наблюдает за вами, чтобы украсть ценную информацию.

h) Вишинг - Это голосовое обращение по телефону (голос+фишинг).

4.

A quid pro **quo** attack is a low-level form of **targeted** hacking that **relies** on human trust. It is also known as a "something-for-something attack". It is a case of **baiting** as attackers **convince** victims to get a service or benefit and the latter performs specific tasks or gives out information or access. An example would be a case of voice **solicitation** when an attacker calls your phone **spoofing** to be from one of your service providers' technical support representatives. They will offer you some assistance that is used to **perpetrate** a scam.

Перевод:

Атака "quid pro quo" (что-то взамен) представляет собой низкоуровневую форму целенаправленного взлома, которая основывается на доверии людей. Она также известна как "что-то взамен". Это случай приманивания, поскольку злоумышленники убеждают жертв получить услугу или выгоду, а последняя выполняет конкретные задачи, предоставляет информацию или доступ. Примером может быть случай голосового обращения, когда злоумышленник звонит на ваш телефон, притворяясь представителем технической поддержки одного из ваших сервисных провайдеров. Они предложат вам некую помощь, которая используется для осуществления мошенничества.

////////////////////////////////////////////////////////////////////////////////////////////////////////

1.

a-phone and internet connection

b-

c-

d-email adress

e-change pass

2.

Protection against phishing:

a) Be cautious about all communications you receive. If it appears to be a suspicious one, do not respond. Delete it.

d) Don't enter personal information in a pop-up screen. Legitimate companies and organisations don't ask for personal information via pop-up screens.

e) Do not click on any links listed in the email message, and do not open any attachments contained in a suspicious email.

f) Install a special spam filter on your email application and your web browser. These filters will not keep out all fraudulent messages, but they will reduce their number.

Protection against vishing:

b) Don't pick up the phone, simply let it go to voicemail. Caller IDs can be faked, which means you might not know who's calling. Later decide whether to call back.

c) Don't press buttons or respond to prompts. Scammers often use these tricks to identify potential targets for more robocalls. And the record of your voice can be used to navigate voice-automated phone menus.

g) Hang up. The moment you suspect it's a fraudulent phone call, don't feel obliged to carry on a polite conversation. Simply hang up and block the number.

h) Verify the caller's identity. If the person provides a call-back number, it may be part of the scam, so don't use it.

3.

Overwhelmed – перегружены

Watchful – бдительны, внимательны

Combo – комбинация

Nefarious – бесчестных, ужасных

Lucrative – прибыль

Purporting – намеревающиеся

Plunder – разграбить

4.

a uses to trick victims

b have been around

c 95 read 45 responded(message)

d 20 read 6 responded(email)

e have become a more attractive attack vector exploiting the more intimate relationship

f revealing credentails

g trick downloading ran wild in

h sending money

I pretending to be a clergyman(священник)

5.

a-cyber attack that uses misleading txt mess to trick victims and installing malware or giving away money

b-users grow more overwhelmed by const email and become less watchful for mess

c-attempts to trick you into revealing credentials, … into downloading malware, … into sending someone money

d-