

# СЪВЕТИ ЗА КИБЕРСИГУРНОСТ

## ПАРОЛИ

Използвайте комбинация от малки и големи букви, цифри и специални знаци. Изберете парола над 10 знака. Не използвайте имена, телефонен номер, рождени дати, повтарящи се или визуално еднакви символи. Не използвайте една и съща парола за няколко различни профила. Не споделяйте паролата си с никого. Запишете паролата си на сигурно място. Сменяйте периодично паролите си. Изберете парола от нашият генератор [ineedpass.com](https://ineedpass.com).

## ФИШИНГ

Игнорирайте имейли или други съобщения от съмнителен източник. Помнете, че държавни институции, банки и фирми почти никога няма да искат от Вас да изпратите лични данни в мейл или чат. Бъдете изключително внимателни при сваляне и активиране на файлове, прикачени към мейли със стресиращ текст или подканящи за незабавно действие.

## ИНВЕСТИЦИОННИ ИЗМАМИ

Доверете се на проверени, доказали се и известни компании и платформи за инвестиции. Не предоставяйте своите имена и телефон на сайтове и инвестиционни платформи, които привидно предлагат висока доходност. Преустановете комуникацията с лица, които постоянно искат да захванват виртуалната си сметка в тяхната платформа, под предлог очакван скок на цени, акции или криптовалута, достигане на определен лимит преди теглене или заплащане на такса за освобождаване на тегленето. Не предоставяйте отдалечен достъп до своя компютър или телефон на непознати лица. Вижте списъка с измамни платформи и сайтове [ТУК](#).

## **ЛИЧНИ ДАННИ**

Не споделяйте лични данни, потребителски имена и пароли, данни от банкови карти или други платежни инструменти при онлайн комуникация, освен ако не сте изрично сигурни къде ги изпращате. Ограничете до минимум информацията, която споделяте за себе си онлайн.

## **НЕ ПОЛЗВАЙТЕ ПИРАТСКИ СОФТУЕР**

Използването на нелицензирани или кракнати програми почти винаги води до рискове от заразяване на Вашето устройство с компютърен вирус. Потърсете безплатна или по-евтина алтернатива на програмата или услугата, която желаете да ползвате.

## **АНТИВИРУСНА ПРОГРАМА**

Изберете съвременна и надеждна антивирусна програма за своите устройства, която редовно обновявайте. Заложете на световноизвестни и проверени решения. Сканирайте редовно своите устройства за киберзаплахи.

## **НАГЛЕЖДАЙТЕ ПАРИТЕ СИ**

Редовно следете движението по Вашите банкови сметки или други виртуални активи. Вземете незабавни мерки, ако установите неоторизиран превод като се свържете с Вашата банка или разплащателна услуга.

## **ОПЕРАЦИОННА СИСТЕМА И ПРОГРАМИ**

Използвайте съвременна операционна система и програми, които редовно обновявайте. Остарелият софтуер по презумпция е по-лесна мишена за хакерите. Проверете настройките на своя компютър или телефон, за да ги обновите до последната версия.

## **АРХИВИРАНЕ**

Регулярно създавайте резервни копия на файлове, чиято съдържание е от особена важност. Съхранявайте тези копия в офлайн среда. По този начин можете лесно да възстановите данните си, ако устройството Ви излезне или стане жертва на рансъмуер.

## **ДВУСТЕПЕННА ВЕРИФИКАЦИЯ/2FA**

Включете опцията за двустепенна верификация, когато това е възможно. Това гарантира допълнителна сигурност за Вашия профил и възможност да си върнете контрола над него при евентуално компрометиране.

## **НЕТИКЕТ**

Комуникирайте учтиво и съдържано онлайн. Не обиждайте и не ругайте. Отнасяйте се с другите, както искате да се отнасят с Вас. Не споделяйте чужди лични данни или снимки, без изрично разрешение. Не разпространявайте снимки или материали с оръжия, наркотици, алкохол, насилие или друго неприемливо. Доверявайте се на надеждни източници на информация и не споделяйте лекомислено фалшиви или непроверени новини.