Правила информационной безопасности

9 правил, которые помогут вам в цифровой жизни!

1. Пароль – как зубная щетка!

Менять надо каждые 2-3 месяца и ни с кем не делиться.

Взлом даже сложного пароля – лишь вопрос **времени**.

Если вы **поменяли** пароль, мошеннику придется начинать подбор с самого начала.

Если у вас один пароль на все сервисы, то взломав самый ненадежный из них, мошенник получит **доступ** ко всему.

2. «На заборе тоже написано»!

Не надо верить всему, что пишут в электронной почте.

Имя отправителя можно **подделать**.

Богатых родственников в Африке, которые могут оставить вам наследство **не существует**.

В лотерею **невозможно выигрывать** каждый день.

Феерические скидки и эксклюзивные предложения, которые действую только сегодня и только для вас – **это лишь уловка**, чтобы заставить вас перейти на зараженный сайт.

3. Данные с карты никому нельзя говорить!

В секрете надо держать не только три цифры на обороте карты, а **все реквизиты карты.**

Для совершения перевода денег достаточно только **16 цифр** на лицевой стороне карты.

Ни срок действия, ни CVV-код, ни имя владельца **не являются обязательными** для совершения транзакции.

Правила информационной безопасности. Владимир Иванов, Coddy © специально для школы семейных финансов «Деньгин's» ® при поддержке Национального центра финансовой грамотности, 2021

4. Двухфакторная авторизация – это не просто смс!

Первый фактор – это то, что вы «знаете», - то, что у вас в голове.

Это невозможно забрать, но можно подсмотреть. Вы не узнаете, подсмотрел кто-то ваш пароль или нет.

Второй фактор – это то, что вы «имеете». Прибор, который физически у вас в руках.

В нем переменные коды, что делает невозможным технологию «один раз подсмотрел и теперь имею доступ».

Его надо буквально украсть, чтобы им воспользоваться. Потерю вы заметите.

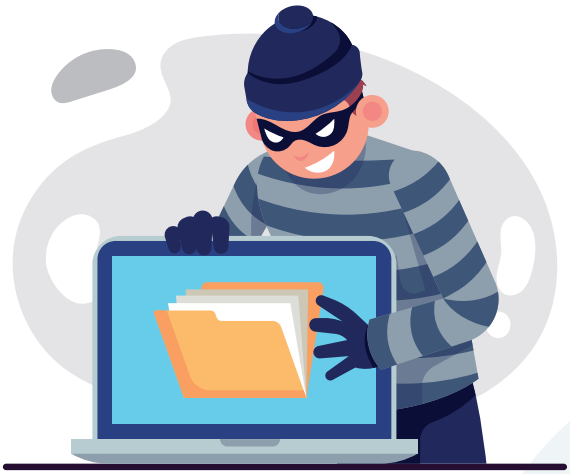
Использование интернет-банка на смартфоне и получение контрольных смс на этот же смартфон сводит **пользу двухфакторной аутентификации к нулю**.

Заведите для **банковских смс** второй телефон.

Самый простой/тонкий/легкий/ с долгой батареей/кнопочный/ неубиваемый.

У вирусов **не будет шансов** его заразить, а значит и похитить ваши деньги.

5. Квартирные кражи всегда осуществляются по наводке



Любой дверной замок можно вскрыть меньше, чем за **2 минуты**. Дверь - за **6 минут**.

Чем **меньше** люди знают, что находится в вашей квартире и в каком количестве, в какой тумбочке вы храните деньги и сколько наличных вы отложили для покупки машины, тем **меньше** шансов на кражу.

6. Номер звонящего человека можно подделать!

Чтобы убедиться, что вам звонит муж/сын/внучка/друг/коллега, задавайте ему **проверочные вопросы**, ответы на которые знает только он/она.

Мошенник может сходу рассказать что-то пикантное, что он уже выведал про вас в интернете.

Опередите его и спросите **«на каком этаже ты живешь?»**.

Что-то очевидное для вас двоих, но неизвестное посторонним.

Два-три вопроса позволят однозначно определить самозванца.

7. Не спешите!

Если вас торопят принять какое-либо решение, то стоит отказаться – это наверняка **плохая сделка**.

И чем сильнее торопят, тем более вероятно, что вас хотят обмануть.

Это работает не только в кибербезопасности, но и при **покупке товаров** в магазине, в выборе новой работы, при оформлении загрантура.

Тот, кому нечего скрывать, не будет вас торопить. Даже в самой экстренной ситуации.

8. Это мой дом, я тут администратор!

Самоутверждаться за счет компьютера **уже не модно.**

Постоянная работа на компьютере должна вестись под **учетной записью пользователя.**

Администратор «включается» только по мере необходимости.

То же самое касается **смартфонов** – не надо его «разлочивать» без необходимости.

Вирусы могут натворить гораздо больше бед, если они, благодаря вам, запустятся **с правами администратора.**

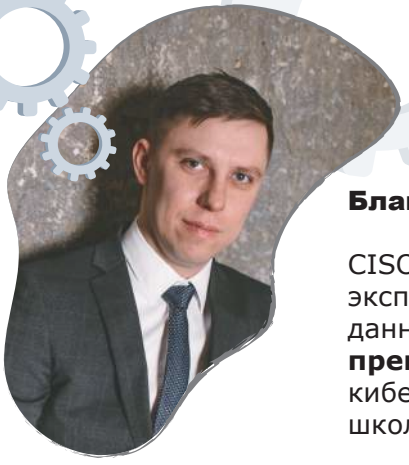
9. Делайте резервные копии!

В случае любого провала, вам будет откуда восстановить данные.

Резервировать можно все!

- *Запасная **карта** с деньгами, которая лежит в номере.*
- *Копия **паспорта** в кармане.*
- ***QR-код** распечатанный + на телефоне + скан в почте, чтобы точно пустили на концерт.*
- *Запасные **ключи** от дома в машине или в офисе на случай, если в кармане оказалась дырка.*
- ***Телефон** лучшего друга вытатуирован на предплечье – чтобы можно было позвонить даже из телефона автомата.*

Оставьте себе шанс на ошибку, дайте возможность **начать все заново.**



Благодарим Владимира Иванова,

CISO в медицинском секторе, эксперта в области персональных данных и финансовой безопасности, **преподавателя** курса по кибербезопасности в международной школе программирования **Coddy**.

https://coddyschool.com/courses/kiberbezopasnost/