Цифровая гигиена

- Гайд по криптобезопасности: как не потерять свои средства, когда пользуешься криптовалютой

Введение

- По мере роста популярности криптовалют растет и активность злоумышленников, которые любыми возможными способами стремятся умыкнуть криптовалюту у холдеров: делая фишинговые атаки, находя уязвимости в исходном коде или представляясь сотрудниками компаний, чтобы получить приватную информацию пользователей, такие как закрытые ключи, пароли, seed-фразы и прочее. Поэтому проблема безопасности при использовании криптокошельков стоит особенно острожно.

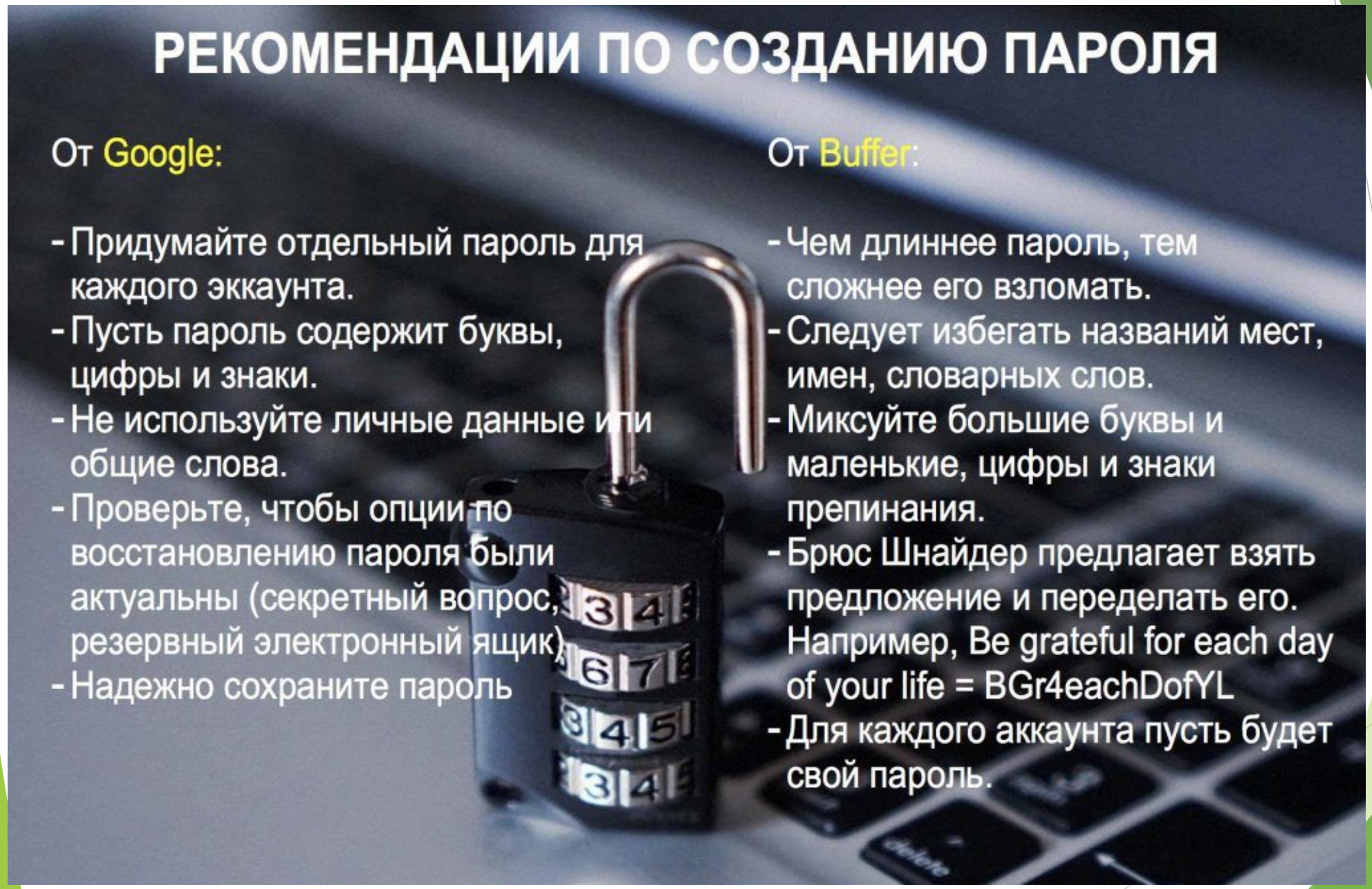
Безопасность почты

- Почта в системе gmail .
- Новое название нигде ее больше не используем
- Для проектов своя, для бирж своя, для кошельков своя.
- Как происходит взлом. Не вас ищут, покупают базы хакеры и уже начинается охота.
- Стиллер (от английского to steal, воровать) — класс по предназначенный для кражи данных с компьютера зараженного. Вирус проникает в хранилище данных популярных программ и ворует данные логинов и паролей, отсылая их злоумышленнику.
- Это касается и приложений на Android. Google Play модерируется намного хуже, чем App Store у iPhone, поэтому мошенники могут опубликовать фейковое приложение.

- При взломе или скаме проекта, будьте уверены ваши данные уже утекли.
- Проверить свою почту на утечку можно на сайте https://haveibeenpwned.com/

- Присланные файлы и ссылки не скачиваем и не переходим по ним если не знаешь что за источник.(Вам оставили наследство переходите заберите)

РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ ПАРОЛЯ



От Google:

- Придумайте отдельный пароль для каждого эккаунта.
- Пусть пароль содержит буквы, цифры и знаки.
- Не используйте личные данные или общие слова.
- Проверьте, чтобы опции по восстановлению пароля были актуальны (секретный вопрос, резервный электронный ящик)
- Надежно сохраните пароль

От Buffer:

- Чем длиннее пароль, тем сложнее его взломать.
- Следует избегать названий мест, имен, словарных слов.
- Миксуйте большие буквы и маленькие, цифры и знаки препинания.
- Брюс Шнайдер предлагает взять предложение и переделать его. Например, Be grateful for each day of your life = BGr4eachDofYL
- Для каждого аккаунта пусть будет свой пароль.

Сложные разные пароли. Да хочется один иметь на все,но это не безопасно. На помощь придут Менеджеры паролей.

https://1password.com/ru/downloads/wi... - 1Password;
https://splikity.com/ - Splikity;
http://www.onesafe-apps.com/ - OneSafe;
http://safe-in-cloud.com/ru/ - SafeInCloud;
https://www.roboform.com/ru - RoboForm;
https://www.dashlane.com/ - Dashlane;
https://www.enpass.io/ - Enpass;
https://www.lastpass.com
https://keepass.info/ - KeePass;
https://www.stickypassword.com/ru/ - StickyPassword
.https://www.dashlane.com -Dashlane
https://nordpass.com -NordPass

Пароли нигде не сохраняем. Ни файл , ни фото . Если распечатал, нужно историю удалять может остаться след.
Хранить на 2х флешках и записать

Зашифруйте свой компьютер и создайте его зашифрованную резервную копию на внешнем носителе информации. Старайтесь придерживаться плана своевременной актуализации резервной копии — неделя-месяц-квартал.
Храните носитель информации с резервной копией в не очень-то доступном для кого бы то ни было месте. Данная мера позволит обеспечить защиту ваших данных: служебных и личных файлов, переписок и различных банковских данных.
Для шифрования достаточно активировать FileVault 2 в вашей MacOS или BitLocker в вашей Windows. Это штатные встроенные средства шифрования, которых вполне достаточно при использовании стойкого пароля.
Учтите, что, если вы забыли пароль для расшифровки, все ваши данные будут безвозвратно потеряны.
Перекинули копию на хард и убрали подальше от чужих глаз.
Используйте antivirus.
Для выхода в сеть можете пользоваться ВПН (Но не все биржи это любят)
https://ru.vpnmentor.com/

соответствующие функции в настройках безопасности аккаунта конкретного сервиса. Ниже ссылки на инструкции по включению 2FA в самых популярных сервисов:
Для идентификатора Apple ID: https://support.apple.com/ru-ru/HT204915
Для Google-аккаунтов: https://www.google.com/landing/2step/?hl=ru
Для Яндекс- паспорта: https://yandex.ru/support/passport/authorization/twofa-on.html
Для аккаунта Mail.ru: https://help.mail.ru/mail/settings/2fa/activate
Для аккаунта ВКонтакте: https://vk.com/@security-dvuhfaktornaya-autentifikaciya-2fa
Для аккаунта в Facebook (ENG): https://www.facebook.com/help/148233965247823
Для аккаунта в Facebook (RU): https://ru-ru.facebook.com/help/instagram/112460429770518 4?helpref=related

Обновляйте ПО компа и телефона. Желательно иметь антивирусник.

Two-Factor Authentication

1. Scan this barcode with your Google Authenticator app:

5TBQOKASYGATBAQV4O7SYYIBB4EOJ5U5

2. Print out this page and store the barcode in a safe place.
Otherwise, there will be no way to regain access to your account if you lose your phone.

3. Type in the pin to confirm:

704670

ENABLE TWO-FACTOR AUTH

В большинстве сервисов 2FA – это использование СМС. Но это не самый безопасный вариант. Поэтому, скачайте и установите приложения типа Google Authenticator или Яндекс.Ключ. Они значительно повысят безопасность.

Устанавливаем 2FA Google auntefícator (При входе проект,биржа просит сохранить QR код. В приложении есть функция сделать импорт и импортируете в новое устройство.

Лайфхак:
Если часто заходишь можно использовать телеграмм Избранное (но при этом не дописать одно слово в сид фразе, Или наоборот лишнее)
Сохранить кошелек под # и закрепить

Используйте многофакторную аутентификацию везде, где возможно. То есть Пин код. Смс подтверждение.

Безопасность связи

И телефон и номер желательно иметь отдельный. С которого вы не будете никому названивать итд.
Использовать для регистраций.
Тариф без аб платы например. Или тот оператор который везде ловит хорошо.
Прийти к оператору и написать заявление что только вы можете заменить сим или выдать дубликат(Могут по поддельной доверенности просто сделать это за вас)
На симку надо поставить PIN-код. оформить у вашего оператора сотовой связи запрет на перевыпуск сим-карты без вашего личного участия.
Примеров из жизни хватает – бизнесмен Данила Бондарь, медиаменеджер Анна Знаменская и т. д... Если интересно – погуглите.

Безопасность в сети

Фишинговые сайты, чтобы не попасть ставим звездочку и в сохраненки.Но всегда просматривать. Убедитесь, что вы совершаете транзакции на защищенном веб-сайте. Его веб-адрес должен начинаться с https://, а не с http://; буква s означает «безопасный» и указывает на наличие у сайта сертификата безопасности. Слева от адресной строки также должен отображаться значок замка. поставить звездочку

Проводить периодически чистку куки история

Безопасность в криптовалютах

- При отправке и получении внимательно смотреть на суммы Пример: отправили 7.008$
- При отправке криптовалюты смотреть на сеть в которой отправляешь (пример он лайн)
- проверка контрагента (кружок в телеграмм,общие чаты или гарант)
- Надежные кошельки с сид фразой Пример .Trast wallet, Coin98

При переводе больших сумм, можно отправить тестово 10 $ Проверить а потом все остальное.

Не хранить крипту в долгосрок (лонг ,холд,ходл) на биржах. Есть аппаратные кошельки (Trezor, Lager)

- Не использовать Wi Fi в чужих местах. Только раздача со своего телефона или проверенная сеть.

Чек-лист (Домашнее задание)

- Прямо сейчас:
- ✓ Завести отдельную карту для покупок в интернете (бирж,проектов, кошельков).
- ✓ Отключить функцию автозаполнения в браузере.
- ✓ Наконец установить менеджер паролей.
- ✓ Создать разные пароли для разных аккаунтов.
- ✓ Установить 2FA везде, где это возможно.
- ✓ Сменить логин и пароль на роутере.
- ✓ Удалить файлы с конфиденциальной информацией и письма с
- восстановлением парольных данных, если есть

Всегда:

✓ Быть осторожным при открытии ссылок и файлов.
✓ Пользоваться официальными магазинами приложений: App Store, Google Play, Windows Market.
✓ Разделять личное и рабочее.
✓ Контролировать доступ приложений к устройству.
✓ Отказываться от автоматического подключения к Wi-Fi.

Регулярно:

✓ Очищать почту от спама.
✓ Сканировать устройства антивирусом.
✓ Создавать везде резервные копии данных.
✓ Менять все пароли.
✓ Удалять ненужные файлы и приложения.
✓ Обновлять ПО всех устройств.
✓ Очищать историю браузера и cookies.

Не подвергайте себя риску, соблюдайте цифровую гигиену электронной почты и своих гаджетов. И помните.Чуть паранойи не помешает

Небольшой инсайд

- Как хранят криптовалюту на очень большие суммы:
- Используют компьютеры, которые никогда не подключали к интернету. У них нет установленной операционки и отслеживающих модулей.
- Создают свой личный VPN
- Ключи хранят в разных местах ,даже странах.(с подтверждением личности)