citizensec

Памятка по информационной безопасности

информация

один из ключевых активов любого бизнеса должен быть надежно защищен.

информационная безопасность

практика предотвращения несанкционированного доступа, использования, раскрытия, изменения или уничтожения информации.

основная задача информационной безопасности

сбалансированная защита конфиденциальности, целостности и доступности данных без ущерба для производительности организации.

подпишитесь на нашу страницу в instagram,
там мы делимся новостями кибербезопасности

citizensec

Содержание

Кибергигиена: защищайте себя каждый день!

90%

успешных кибератак начинаются с ***фишингового письма***.

обязательно проверьте ссылку перед тем, как нажать на нее!

интернет-трафика генерируется ***программами*** и ***ботами,*** которые могут представлять угрозу безопасности

>50%

300,000

новых вредоносных программ создаются в мире ***каждый месяц***.

будьте уверены, что ваш ***антивирус обновлен!***

человек становится жертвой хакеров из-за ***слабых паролей***.

используйте ***менеджеры паролей*** для повышения безопасности!

1/5

~60%

пользователей откладывают ***обновления ПО***, что увеличивает вероятность быть взломанным

// пока вы прочитали этот текст, в мире произошло **более 30 кибератак**

Правила создания и использования паролей (1/3)

1 используйте уникальный пароль для каждого аккаунта, электронной почты

Марк Цукерберг использовал одинаковый пароль для всех соц.сетей. Из-за этого хакеры в 2016 году получили доступ к его аккаунтам. Результатом было падение акций Facebook.

Учитесь на ошибках других, не делайте как Марк.

2 пароль должен содержать не менее 14 символов

Взлом пароля — это перебор вариантов, чем их больше, тем сложнее взломать пароль.

Усложните жизнь хакеру сделав свой пароль длиннее.

3 включает буквы верхнего и нижнего регистров, цифры и знаки пунктуации

a-z, A-Z

0-9, !@#$%^&*( )_+|~-=\{ }[[ ]:«;'<>?,./

4 не является словом на любом языке, диалекте, сленге, жаргоне и т.д.

Запомните, пароль аткси1387 _1 всегда будет более надежным, нежели такси1387_1.

Это классика, это знать надо!

5 не основан на персональной информации, н-р, фамилии, дате рождения, номере тел.

Хакеры могут предугадать ваши пароли на основе собранной информации о вас.

Полная анонимность - ваше всё.

6 хранение и передача пароля только через корпоративный менеджер паролей.

Запрещено хранение и передача паролей другими способами.

Very demure, very mindful.

Правила создания и использования паролей (2/3)

7 везде включить двухэтапную аутентификацию

Усложните жизнь хакеру еще больше, ведь при многофакторной авторизации ему понадобится доступ к еще и другим данным.

Где-то в мире плачет один хакер.

8 каждые 90 дней - новые пароли ко всем аккаунтам

Вбейте в Google Calendar процедуру смены паролей.

Обновление - мать учения.

9 подпишитесь на оповещения о несанкционированном доступе и меняйте пароли от взломанных аккаунтов (firefox monitor или haveIbeenPwned).

Вам сразу же придет оповещение, как только произойдёт утечка базы данных, где будут замечены ваши данные.

Вам будет необходимо сразу сменить свои пароли.

Рекомендуется генерировать пароли в *Dashlane*.

Выставив указанные на предыдущей странице правила можно сгенерировать пароли.

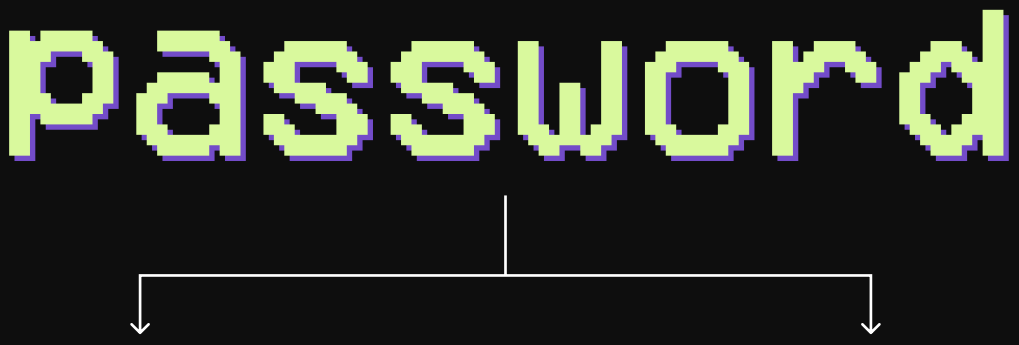
Правила создания и использования паролей (3/4)

Использование ***надежных паролей*** далеко не такой простой вопрос, как может показаться с первого взгляда.

И, давайте признаем, хоть мы все и знаем требования к надежному паролю,
чаще все-таки пользуемся простыми, так как их легко запомнить.

?

А вы знали, что самый распространенный пароль в мире - это ‘123456’?



Высокая степень сложности

1. дешифрование жесткого диска
2. доступ к менеджеру паролей
3. доступ к рабочему криптоконтейнеру

Обычная степень сложности

1. веб-сайты
2. почты
3. мессенджеры

Правила создания и использования паролей (4/4)

К сожалению, многие используют пароль не только ненадежный, **но и один пароль на нескольких ресурсах**.

Некоторые ресурсы специально созданы для сбора логинов и паролей.

Представим ситуацию:

1 *Вы зарегистрировались на интересном вам сайте.*

2 *Ввели email и пароль, а сайт принадлежит злоумышленникам, и все данные попадают к ним в руки.*

3 *Они проверяют не подходит ли указанный пароль к вашей почте.*

4 *Пароль подошел и теперь ваша почта принадлежит злоумышленникам.*

// мем смешной, ситуация страшная

Про фишинг и как его распознать (1/2)

Фишинг

вид интернет-мошенничества, цель которого — кража идентификационных данных пользователей

Цель: Заставить жертву перейти по ссылке и ввести личные данные.

Угроза: Современные атаки становятся более продуманными благодаря методам социальной инженерии.

Когда придумали фишинг?

интересный факт

Техника фишинга была подробно описана в 1987 году, а сам термин появился 2 января 1996 года в новостной группе alt.online- service.America-Online сети Usenet, хотя возможно его более раннее упоминание в хакерском журнале 2600.

Обычно под фишинговой атакой подразумевается **пришедшие на почту поддельные уведомления/сообщения**, целью которой является заставить жертву перейти по ссылке в теле письма и ввести чувствительные данные (пароль, код итд).

Сегодня атаки фишеров становятся все более продуманными, применяются методы социальной инженерии.
Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию.

Будьте осторожны!

Про фишинг и как его распознать (2/2)

Фишинг сегодня или какие виды фишинга существуют?

1. *звонки на телефон*
   Вишинг
2. *встроенная вредоностная программа*
   Малвертайзинг
3. *поддельные письма и ссылки*
   Фарминг
4. *рассылка писем*
   Спам-фишинг
5. *фейковые сайты*
   SEO фишинг
6. *СМС, сообщения*
   Смишинг (SMS phishing)
7. *целенаправленный фишинг*
   Целевой фишинг (Spear phishing)

! *Фишинговые атаки становятся всё более реалистичными и сложными для распознавания, что некоторые современные фишинговые сайты на 99% похожи на реальные.*

Распространенные ошибки и как их избежать

1 не использовать антивирусную защиту

Установите антивирус на все устройства — он защитит от *спама*, *фишинга* и *кражи данных*.

2 переходить по ссылкам из сообщений от незнакомых адресатов

Мошенники используют адреса, похожие на реальные, например, вместо *mail@technodom.kz* пишут *mail@technodon.kz.*

Всегда проверяйте адрес: даже небольшие отличия указывают на подделку.

3 не проверять адресную строку сайта

Адрес. Лучше всего сохранять адреса в закладках.

Это не паранойя, это информационная безопасность. Не путайте.

4 платить через небезопасные страницы

Запомните, официальные банки переводят вас на безопасные страницы и отправляют одноразовый код для подтверждения платежа.

5 использовать одну и ту же карту для всех платежей

Для онлайн-покупок лучше завести отдельную карту и переводить на нее ровно ту сумму, которая нужна для платежа.

О проекте

citizensec.kz

- это социальная инициатива, направленная на ***повышение уровня кибербезопасности*** в Казахстане.

Наша миссия — сделать кибербезопасность ***доступной*** для каждого.

Мы стремимся помочь обществу ***осознать угрозы*** в цифровом мире и научиться эффективно ***защищаться*** от них.

Кому это нужно?

1. **Частным лицам:**
   Защита личных данных и конфиденциальности в интернете.
2. **Малому и среднему бизнесу:**
   Устойчивость к кибератакам, защита корпоративной информации.
3. **Образовательным учреждениям:**
   Подготовка студентов и преподавателей к грамотному использованию технологий.

Что мы предлагаем?

1. **Обучающие программы и семинары:**
   Практические советы и знания для различных уровней подготовки.
2. **Консультации по кибербезопасности:**
   Персонализированные рекомендации для частных лиц и организаций.
3. **Онлайн-курсы и вебинары:**
   Удобные форматы обучения по актуальным темам.
4. **Партнерские проекты:**
   Взаимодействие с правительственными и негосударственными организациями для повышения уровня кибербезопасности в Казахстане.

Мы помогаем понять, как защитить себя в этом цифровом мире

по вопросам
info@citizensec.kz

вебсайт
https://citizensec.kz

контент
@citizensec.global