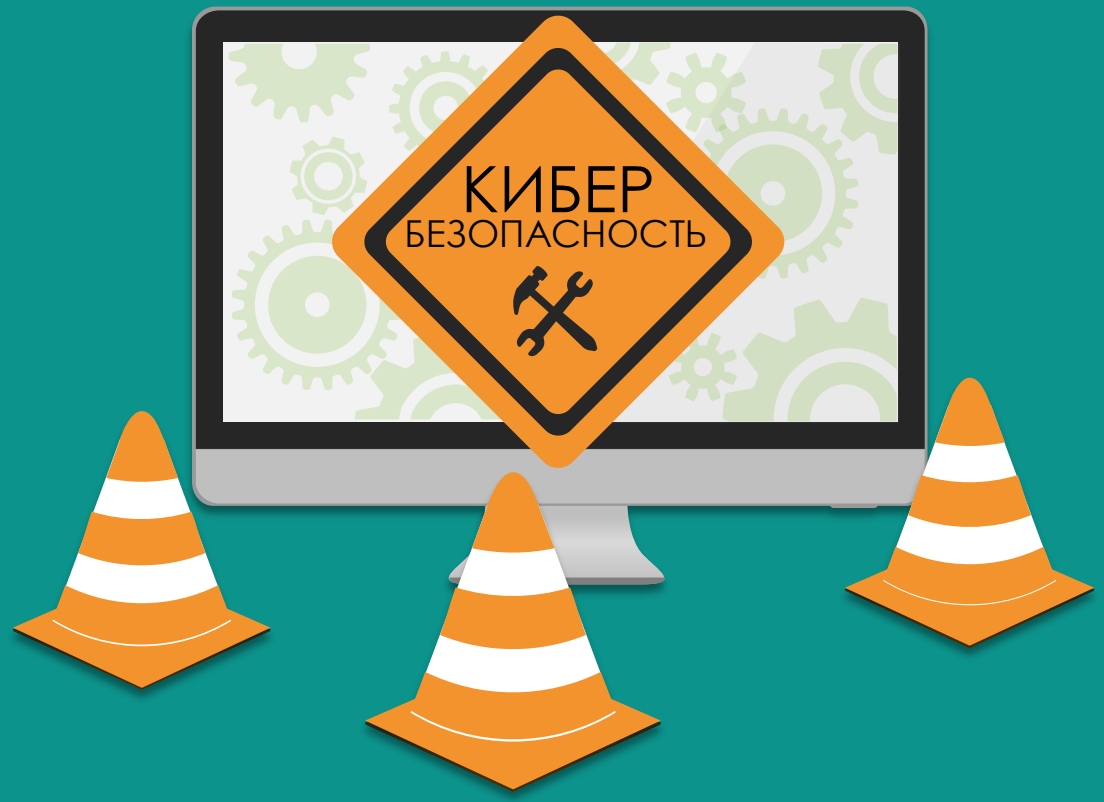

КИБЕРГИГИЕНА

Кибербезопасность РГП «ГРС» дело общие

САТЫБАЛДИЕВ ҚОЗЫКЕ

Главный специалист по информационной безопасности

Тел.: 87786275049
Эл. почта: q.satybaldiyev@rfs.gov.kz

Под информационной безопасностью подразумевают соблюдение трех важных принципов:

Конфиденциальность

Что это такое? Доступ к информации должен быть только у того, кто имеет на это право. А у кого нет права, тому доступ к информации закрыт.

Плохой пример: Доступ к номеру Вашей карточки и CVV коду заполучил плохой человек.

Что это такое? Информация должна быть доступна в любой момент, когда она нужна. Сразу и быстро.

Доступность

Плохой пример: Вы должны подать заявку на устройство ребенка в детский сад через Портал Акимата. По-другому не принимают. Но сайт этого портала не открывается. 5 минут, 15 минут, час, день, неделю...

Что это такое? Информация должна быть достоверной. Она не должна меняться сама и тем более ее не должны искажать намеренно.

Целосность

Плохой пример: Вы делаете перевод денежных средств со своей карточки на карточку друга. Вредоносное ПО может изменить номер карточки получателя и отправить деньги на карточку злоумышленника.

6 шагов к личной информационной безопасности

Шаг 1:

Храните ЭЦП как ЗЕНИЦУ ОКА

Получить ЭЦП легко, но есть серьезная опасность! Если ЭЦП украли, то документы за Вас могут подписывать кто-то другой.

Что делать?

1. Самое надежное спрятать Ваше ЭЦП в надежное хранилище. Таким хранилищем является электронный чип, что установлен во всех удостоверениях личности нового образца граждан РК.
2. Также можно воспользоваться специально хранилищем, которое называет ТОКЕН.

Что не нужно делать!

1. Никогда не отправляйте ЭЦП в открытом виде по электронной почте.
2. Никогда не копируйте свое ЭЦП на незнакомые компьютеры.
3. Не храните свое ЭЦП на компьютере.

ШАГ 2

Ваш ЩИТ – Ваш ПАРОЛЬ

Что делать?

1. Садясь за рабочий компьютер, оглядитесь вокруг. Вокруг Вас будут сотни предметов, которые постоянно находится на Вашем столе, на стенах, в шкафах или даже за окном. Пример: Zelenyi_kaktus
2. Использовать символы, цифры, буквы верхного и нижного реестра

Что не нужно делать!

Ваш ЩИТ – Ваш ПАРОЛЬ

1. Никогда не передавайте свои пароли другим людям.
2. Не записывайте свои пароли на стикеры, бумажки.
3. Не храните пароли в электронной почте.
4. Не храните пароли в автозаполнении.

ШАГ 3

Электронная почта

Что делать?

1. Никогда не открывайте самозапускаемые файлы.

Пример: .exe , .com , .cmd , .msi , .bat

Файлы вложений с такими расширениями открывать нельзя!

Что не нужно делать!

Электронная почта

1. Не открывайте подозрительные письма.
2. Не отвечайте на подозрительные письма.
3. Не переходите по ссылкам в подозрительных письмах.

ШАГ 4

Обновления и еще раз обновления

Что делать?

1. Устанавливать овновления программного обеспечения.
2. Проверять, установлены ли последние овновления.

Что не нужно делать!

1. Использовать пиратское программное обеспечение.
2. И, пожалуйста, не отключайте обновления.

ШАГ 5

Социальная инженерия. Социальные сети.

Социальная инженерия – метод получения необходимого доступа к информации, основанной на особенностях психологии людей.
Социальные сети могут быть источником излишней информации о Вас!

Что делать?

1. Будьте внимательны, собраны и осторожны.

Что не нужно делать!

1. Разговаривать с незнакомыми людьми по телефону насчет своих банковских счетов или карт.
2. Не отвечать на подозрительные письма, но об этом мы уже говорили в разделе ПОЧТА.
3. Отдавать свою карточку официанту или бармену надолго на руки. Платите картой только сами.

ШАГ 6

Резервное копирование

Информация может исчезнуть. И не обязательно Вас атаковали злые хакеры. Просто потеряли телефон или сгорел жесткий диск компьютера.

Что делать?

1. Регулярно копировать важную информацию на внешний носитель.

Что не нужно делать!

1. Хранить в облаке очень конфиденциальную информацию все же не стоит. ЭЦП не стоит хранить в облаке.

Спасибо за внимание!

Тест: В кибербезопасности ли вы?

1. Поговорим о паролях. Какой из них надежный?

1) 13051998
2) satybaldiyev95
3) $uper#Parol@314

2. **Сколько у вас паролей?**

1) Один, память же не резиновая.

2) Двух хватает. Один простенький, другой - для тех сайтов, которые говорят, что он ненадёжный.

3) Свой пароль для каждого сайта.

3. Вам на почту пришло письмо, в котором говорится, что вы выиграли айфон и для этого нужно перейти по ссылке! Что будете делать?

1) Конечно перейду по ссылке, новый айфон не помешает.

2) Не буду переходить, выглядит как развод.

3) Вспомню, что хорошего случалось со мной за последнее время, если ничего - то, может, и правда повезло.

4. А двухфакторной аутентификацией пользуетесь?

1) Нет, а это что?

2) Нет, зачем оно мне надо

3) Конечно, так злоумышленники не смогут получить мои данные.

5. Что может привести к заражению компьютера?

1) Получение сообщения по электронной почте
2) Загрузка пиратского ПО
3) Создание нового файла
4) Отправка сообщения по электронной почте

6.Безопасно ли сохранять пароли в автозаполнении браузера?

1) Да, если пароль к входу в систему знаю только я один
2) Нет
3) Да, если этим компьютером пользуюсь только я один
4) Да

7. Что необходимо выполнять для контроля безопасности электронной почты?

1) Часто сменять пароли

2) Проверять страницу посещения

3) Регистрировать почтовый ящик только в известных системах

4) Использовать сложные пароли