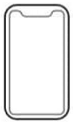
БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ

Компьютер

- Создайте сложный пароль
- Работайте только под своей учётной записью
- Шифруйте данные на вашем устройстве (FileVault на MacOS / BitLocker на Windows)
- Блокируйте экран, когда отходите от компьютера



Мобильный телефон

- Создайте сложный пароль
- Отключите уведомления при заблокированном экране
- Отключите синхронизацию с другими устройствами

АНОНИМНОСТЬ И БЕЗОПАСНОСТЬ

Используйте VPN

сервис имитирует ваш выход в интернет с чужого компьютера

Очищайте метаданные

Это информация в документах и изображениях о том, кем, когда, где и каким оборудованием они были созданы

Используйте средства анонимной передачи информации

мессенджеры, временная почта Temp-mail, пароли с архивом и т.д.

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Установите двухфакторную аутентификацию

Проверьте/установите облачные пароли

и контакты для восстановления к сервисам

Контролируйте активные сессии

Выходите из своих аккаунтов после работы. Если «был выполнен подозрительный вход с чужого устройства», то завершите этот сеанс на вашем устройстве

ФИШИНГ

Это мошеннический способ получения доступа к вашим личным данным, банковскому счёту, архивам со служебной информацией и т.д.

Примеры сообщений

Ваша учетная запись была или будет заблокирована/отключена

В вашей учетной записи обнаружены подозрительные или мошеннические действия

В вашей учетной записи требуется обновление настроек безопасности

Требуется подтвердить право владения учетной записью

Вы получили важное сообщение. Перейдите в личный кабинет

Особого внимания требуют письма, которые содержат

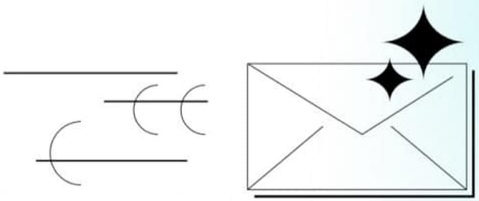
- Ссылку для перехода на сторонний ресурс
- Подозрительный прикреплённый файл

КАК ОБНАРУЖИТЬ ФИШИНГОВОЕ ПИСЬМО?

Критически оценивайте каждое входящее письмо!

Задайте себе следующие вопросы:

- Ожидаю ли я это письмо?
- Есть ли смысл в том, что от меня требуют?
- Знаю ли я автора этого письма?
- Если я сделаю, что от меня требуют – какие могут быть последствия?



КАК ОБНАРУЖИТЬ ФИШИНГОВОЕ ПИСЬМО?

2. Внимательно проверьте отправителя

- Проверить полное имя отправителя письма

Пример

ivanova@gosuslugi.ru – корректный

ivanova@gocuslugi.su – ложный

3. Посмотрите на содержание письма

Если в письме есть кнопки, слова-ссылки или картинки, наведите мышкой на них и в левом нижнем углу вы увидите настоящую ссылку, которая скрывается под ними

4. Файлы-вложения

Не скачивать и не запускать файлы если вы:

- не ожидаете получить подобный файл от данного отправителя
- не знаете отправителя файла
- не знаете какой программой открыть полученный файл

Ни в коем случае не запускать макросы в офисных приложениях !

КАК ОБНАРУЖИТЬ ФИШИНГОВОЕ ПИСЬМО?

1. Анализируйте гиперссылки

- Знаком ли вам сайт, на который вам предлагают перейти в письме? Корректно ли записано имя сайта, на который вам предлагают перейти?

Пример

https://mail.google.com/mail – корректный

https://mailgoogle.com/mail – ложный

- Корректно ли записан домен верхнего уровня?

Пример

https://gosuslugi.ru – корректный

https://gosuslugi.su – ложный

- Наличие коротких гиперссылок

Пример

htps:/bit.ly/2sAHAOv

htps:/cut.ly/wrwtLNH

ЧТО ДЕЛАТЬ ЕСЛИ ВЫ ОБНАРУЖИЛИ ФИШИНГОВОЕ ПИСЬМО?

- Не переходить по ссылке
- Не копировать адрес ссылки
- Не скачивать документы из письма
- Не открывать их
- Не пересылать письма коллегам
- Не использовать телефон для перехода по ссылке
- Не подгружать картинки от незнакомых людей
- Если вы считаете, что ваши учётные данные стали доступны злоумышленникам, срочно меняйте их

ПАРОЛЬНАЯ ПОЛИТИКА

1. Криптостойкий пароль

Например, меняем все буквы «е» на цифры по порядку, буквы «с» на %

Было	Стало
«Ваше политическое кредо? Всегда! Россия вас не забудет»	Ваш1 политич2%ко3 кр4до? В%5гда! Ро%%ия ва% н6 забуд7т!

Как вариант, пишем русские слова английской раскладкой:

Dfi1gikbnbx2%rj3rh4lj?D%5ulf!Hj%%bzdf%y6pf,el7n!

2. Одно устройство – один пароль

3. Не используйте личные данные (свои и родных) в пароле

КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ

1. **Не используйте открытые носители для хранения паролей**

   в ленте или на своей странице в соцсетях, а также на стикерах около компьютера, на обратной стороне телефона и т.д.

2. **Используйте парольные менеджеры**

   специальные онлайн-сервисы для надежного хранения паролей. Например,LastPass, 1Password или Dashline

3. **Ставьте только официальное ПО**

   пиратские программы опасны и не поддерживаются производителем. Их установка может привести к взлому