ИНФОРМАЦИОННАЯ ПАМЯТКА ПО ВОПРОСАМ КИБЕРБЕЗОПАСНОСТИ

ОСНОВНЫЕ ПРАВИЛА ПО СОБЛЮДЕНИЮ ЦИФРОВОЙ ГИГИЕНЫ

1. Передавать служебную информацию и документы только через корпоративную почту и систему внутреннего документооборота
2. Использовать надежные пароли: не менее 8 символов, буквы верхнего и нижнего регистров, цифры и специальные символы
3. Использовать двухфакторную аутентификацию: логин и пароль плюс код из СМС, push-уведомления или почты
4. Использовать различные надежные пароли отдельно для каждого ресурса
5. Обращать внимание на адресную строку, переходить на сайт только по известному имени ресурса
6. Устанавливать программное обеспечение из официальных источников (магазинов приложений)
7. Использовать доверенные сети для доступа к личным кабинетам, мессенджерам, электронной почте
8. Использовать проверенные съемные носители (flash-накопители)
9. Работать с установленным и обновленным антивирусом
10. Использовать информацию, полученную только с официальных сайтов государственных органов
11. Следить за своевременным обновлением операционной системы, приложений, антивирусных баз

ЗАПРЕЩЕНО:

- Передавать служебную информацию и документы через сеть Интернет - открытые почтовые сервисы, мессенджеры, социальные сети
- Использовать простые пароли, состоящие только из букв или цифр, не содержащие спецсимволы
- Использовать публичные компьютеры для подключения к личным кабинетам, мессенджерам, электронной почте
- Использование без предварительной проверки неизвестных flash-накопителей
- Работать без антивирусной защиты

ПРАВИЛА ПОВЕДЕНИЯ ПРИ ПОЛЬЗОВАНИИ ТЕЛЕФОННОМ И МЕССЕНДЖЕРАМИ:

- Всегда критически воспринимайте информацию, которая вам поступает – голосом, видео или текстовым сообщением
- Никогда не сообщайте свои личные данные, данные банковских карт, писем, смс-сообщений
- Убедитесь, что вы общаетесь именно с этим собеседником, если есть возможность, отложите разговор и свяжитесь с ним альтернативным способом, во время разговора используйте дополнительные способы проверки – задавайте вопросы, ответы на которые известны только вам и собеседнику
- Во время разговора помните, что современные технологии позволяют подделывать голос и изображение, создавая иллюзию общения со знакомым или близким вам человеком
- Имейте всегда в виду, что озвученная во время разговора информация может попасть в руки мошенников
- Если звонят из банка, уточните имя оператора (личный номер) и перезвоните ему самостоятельно через номер контакт-центра банка. Помните, что специалисты банка не звонят клиентам, используя мессенджеры, и никогда не просят сообщить им данные карты, поступившего или смс-сообщения. В случае любого сомнения сразу прекратите общение
- Всегда внимательно вводите коды подтверждения при оплате товаров и услуг в интернете, всегда читайте в смс-сообщении, оплату чего вы производите
- Установите лимиты на списание с банковских карт и на оплату покупок в интернете
- При получении смс-сообщений с одноразовыми паролями, пин-кодами, ссылками никому их не сообщайте и не переходите по ссылкам

ЧТО ДЕЛАТЬ, ЕСЛИ…

Утерян (украден) мобильный телефон	Заблокировать SIM-карту, позвонив на горячую линию своего оператора связи Заблокировать (приостановить) доступ к банковским картам Обратиться к оператору связи для получения новой SIM-карты Оповестить коллег, знакомых, что с вашего номера мошенники могли направить сообщения
Утерян (скомпрометирован, т.е. стал известным посторонним) пароль для доступа в личный кабинет портала Госуслуг, вашего банка и к другим информационным ресурсам	Произвести смену пароля с учетом требований надежности, активировать двухфакторную аутентификацию При невозможности получения доступа к ресурсу сообщить в службу технической поддержки / системному администратору
Вы получили сообщение о доступе в личный кабинет, который вы не производили	Сменить пароль доступа, обратиться в службу поддержки портала, информационного ресурса