Памятка для пользователей по кибергигиене

Кибербезопасность *— это набор процессов, рекомендаций и технологий, которые помогают предотвратить несанкционированный доступ к критически важным системам.*

Пользователям не рекомендуется:

1. Открывать неизвестные письма из внешних почтовых сервисов (mail.ru, yandex.ru, gmail.com и др.), СМС, сообщения в мессенджерах и переходить по ссылкам, доверять и передавать им запрашиваемую ими информацию.
2. В случае отсутствия достаточной уверенности в надежности источника и/или прикрепленного (вложенного) файла открывать или запускать файлы (*.pdf, *.bat, *.exe, *.com, *.doc, *.xls, *.jr, .exe, .com, .bat, .cmd) и файлы-архивы (.rar, .zip, .tar, .arj и др.), прикрепленные к почтовым сообщениям, а также загружать в сеть Интернет и распаковывать из сети Интернет и электронной корпоративной почты на ПК прикрепленный (вложенный) файл без предварительной проверки на наличие вредоносного кода.
3. Хранить пароли на доступных для чтения без авторизации носителях (например, на бумаге, в текстовом файле и т.д.).
4. Оставлять устройства разблокированными и без присмотра.
5. Загружать, публиковать и распространять материалы, содержащие логины, пароли и прочие средства для получения несанкционированного доступа к информационным ресурсам, а также ссылок на информацию о несанкционированных доступах к ним.
6. Передавать свои пароль и логин для доступа к информационным системам или устройству.
7. Сохранять (кэширование) на устройствах пароли на доступ к информационным ресурсам и различным информационным сервисам. При использовании браузера на устройстве предложения о сохранении логина и пароля необходимо отклонять.
8. Использовать сеть Интернет в целях передачи и распространения материалов, содержащих конфиденциальную информацию.

1) посещать сомнительные и вредоносные сайты;
2) загружать (передавать) вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;
3) использовать службы интернет-чатов, коммуникаторов.

Пользователям рекомендовано:

1. **Храните пароли в безопасности**

- Не используйте один и тот же пароль для разных сайтов и сервисов.
- Регулярно (1 раз в 3 месяца) меняйте пароли.
- Используйте пароли длиной не менее 12 символов (чем длиннее, тем лучше).
- В состав пароля должны входить заглавные и строчные буквы, символы и цифры.
- Не используйте комбинации последовательных цифр (1234) и личную информацию, которую можно угадать: например, дату вашего рождения или имя домашнего животного.
- Меняйте установленные по умолчанию пароли.
- Не записывайте пароли на бумажку и не сообщайте их другим людям.
- Используйте менеджер паролей, чтобы создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

2. **Многофакторная аутентификация**

- Настройте защиту с использованием многофакторной аутентификации для всех основных учетных записей (электронная почта, социальные сети, банковские приложения) с помощью таких приложений, как Google Authenticator или Authy.
- Сохраняйте резервные коды многофакторной аутентификации в диспетчере паролей.

3. **Обеспечение конфиденциальности**

- Не публикуйте в социальных сетях личную информацию: свой домашний адрес, фотографии, номер телефона, номера кредитных карт.
- Убедитесь в том, что настройки конфиденциальности в соцсетях установлены на комфортном для вас уровне.
- Избегайте участия в викторинах, играх и опросах в социальных сетях, где запрашивают конфиденциальную личную информацию.
- С осторожностью одобряйте доступы к вашим данным, которые запрашивают различные приложения.
- Заблокируйте компьютер и телефон с помощью пароля или PIN-кода.
- Не работайте с личной информацией при подключении к общедоступным сетям Wi-Fi.
- Виртуальная частная сеть (VPN) поможет обеспечить максимальную конфиденциальность, особенно при подключении к общедоступным сетям Wi-Fi.
- Проводите интернет-платежи, бронирование билетов и оставляйте персональные сведения только на безопасных веб-сайтах, веб-адреса которых начинаются с **https://**, а не с http://, а слева от адресной строки виден значок замка.
- Рассказывайте о правилах кибербезопасности своим близким и друзьям, чтобы они также могли их внедрить.

4**. Обновление приложений и программного обеспечения**

- Регулярно обновляйте приложения, веб-браузеры, операционные системы и прошивки, которыми пользуетесь. С обновлениями загружается их улучшенный функционал, в том числе, в сфере безопасности.
- Настройте функции автоматического обновления ПО.
- Удаляйте неиспользуемые приложения.
- Загружайте приложения только из надежных и официальных сайтов.

5. **Защита от атак социальной инженерии**

- Не переходите по подозрительным ссылкам, которые получили по почте или в мессенджерах от неизвестных адресатов. Не переходите по ссылкам, которые приходят от друзей в соцсетях без описания или с текстом на латинице, часто хакеры взламывают чужие профили и рассылают опасный спам.
- Не открывайте письма, которые выглядят подозрительно.
- Не загружайте незнакомые и подозрительные вложения из сообщений электронной почты, а также текстовые сообщения, которых не ждали.
- Не переходите по ссылкам в объявлениях, которые обещают бесплатные призы, деньги или скидки.

6. **Надежная антивирусная защита**

- Используйте надежное антивирусное ПО на ваших гаджетах. Оно выполняет проверку устройств на вирусы и прочие вредоносные программы и удаляет опасные.
- Постоянно обновляйте антивирусное ПО.