Правила кибергигиены

Создавайте надежные пароли. Что делает пароль надёжным:

- Длина пароля 10 или более символов
- Использование верхнего и нижнего регистра, чисел и символов
- Использование случайных комбинаций
- Отсутствие простых комбинаций букв и чисел
- Отсутствие публичной информации

Подключите двухфакторную аутентификацию:

- 1 этап – стандартные логин и пароль
- 2 этап – код, который приходит пользователю в СМС, push-уведомлении или почте.

Где использовать? На всех ресурсах, где содержатся важные данные или совершаются финансовые операции: при входе в аккаунты социальных сетей, порталы государственных услуг, интернет-банкинг и прочие.

Будьте внимательны к письмам со ссылками и файлами.
Как определить фишинговое письмо:

- Оцените содержание
- Проверьте автора письма
- Наведите курсор на ссылку в сообщении
- Оцените вложенный файл

Будьте внимательны к именам сайтов или отправителям писем
Как определять фишинговый сайт:

- Внимательно проверьте, что адрес сайта написан верно – мошенники могут заменить всего одну букву.
- Обратите внимание, что домен указан верно — иногда фишинговые сайты размещают в домене .su, .org и прочих вместо .ru, тогда как сам адрес до точки остается тем же.
- Иногда письма присылают с адреса типа bank@mail.ru. Помните, что организации не присылают письма с адресов общедоступных почтовых сервисов: @mail.ru

- Совет: Лучше ввести адрес сайта вручную и найти интересующий вас раздел с акцией или другой информацией.

Не скачивайте файлы из непроверенных источников.
Под видом бесплатных программ (особенно, дорогих) мошенники могут замаскировать зловредное ПО. Задачами такого ПО могут быть: кража ваших данных (логинов, паролей, фото, контактов), перехват любой вводимой на устройстве информации, подписка на платные услуги, сбор информации в рекламных целях.