

Как не стать жертвой мошенников в сети

1. Источник информации
2. Общение по сети, социальные сети
3. Образование
4. Покупка в интернет-магазинах
5. Медиа-контент: фильмы, книги и др.

Преимущества сети Интернет

1. Недостоверная информация
2. «Подложные» друзья в социальных сетях
3. Образование может быть не качественным
4. Опасность утечки данных: паролей, банковской карты, взлом почты.

Риски: фишинговые сайты, фальшивые страницы банков и даже Банка России в соцсетях, где якобы разыгрываются призы или выплачиваются компенсации

Опасности сети интернет

Опасность: вирус

Не переходите по «странным» ссылкам и всплывающим окнам



Опасность: похищение денег при оплате в сети

Обращайте внимание на адресную строку,
замок означает безопасное соединение

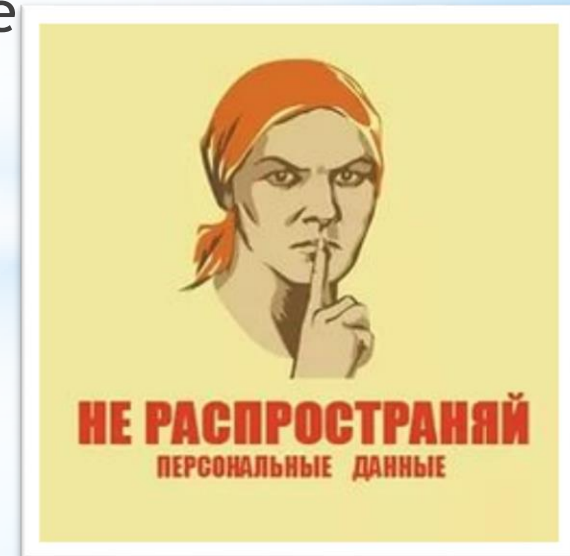


Опасность: похищение персональных данных

МИФ: да кому они нужны, мои данные?

Звонки из так называемых служб безопасности банков

Банки, почтовые сервисы НИКОГДА не просят ваши данные. Они им НЕ НУЖНЫ, ибо и так у них имеются. Просить номер карты, данные паспорта, где вы работаете могут только МОШЕННИКИ





Опасность: получение фишингового письма

Перед просмотром входящих писем на электронном ящике, проверьте адрес отправителя . Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.

Пример: письмо от Google

Подтвердите данные вашего аккаунта, в противном случае он будет удален в течение 30 минут.

Что делать? - Удалить письмо

или - Посоветоваться с друзьями

или - Написать в Гугл

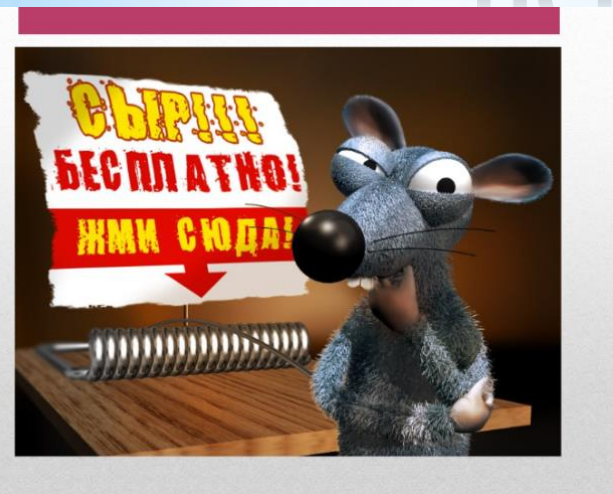
Цель мошенников: украсть ваши деньги или получить ваши данные и с их помощью украсть ваши деньги

Узнав пароль, мошенник может:

- * Разослать от вашего имени письма (например, угрозы)
- * Разослать сообщения в соцсетях
- * К адресу почты привязаны другие аккаунты: соцсети, онлайн банк и тп. Таким образом, мошенник получит доступ к смене пароля в других аккаунтах
- * Получить доступ к вашему онлайн банку.

**Опасность:
похищение пароля**

Мошенники используют психологический подход



- * Используют социальную инженерию - психологический подход к обману. Например, звонит кто то авторитетный.
- * Оставляется крайне мало времени на размышления, например, письмо с лотерей

ПОМНИТЕ! Ни представители почтовых сервисов, ни представители соцсетей, ни тем более банков НИКОГДА не просят ввести ваши данные. Это нужно только **МОШЕННИКАМ**

Безопасность пароля

- * Используйте разные пароли для разных сервисов
- * Делайте сложный пароль: 8 знаков, буквы прописные и строчные, цифры. Используйте генератор паролей.
- * Не сообщайте ваш пароль даже близким, возможен случайный ущерб.
- * Лучше всего пароли запоминать.
- * Никогда не храните пароль в том виде, в каком вы его используете.
- * Используйте двухфакторную идентификацию

Безопасность пароля

Безопасно хранить пароль с помощью записи напоминания. Запись-напоминание - любая запись, которая поможет вам вспомнить пароль.

ПРИМЕР: пароль lion271kiTTen

ЗАПИСЬ: лев172котенок

ЗАПИСЬ: lion271

ОПАСНОСТЬ: записать пароль, имя пользователя и от чего он

Безопасность пароля

Где хранить бумажку с напоминанием пароля?

**Храните пароль в месте, к
которому вы относитесь
внимательно**

- * При первом подозрении срочно смените пароль.
- * Время - ключевой фактор. Чем дольше вы не меняете пароль, тем больший ущерб могут причинить мошенники

Что делать, если кто-то узнал мой пароль?

Признаки взлома аккаунта

Признак 1: сообщение из аккаунта

В ваш аккаунт была попытка входа в 11.13. Это были вы?

Вы не знаете, была ли попытка входа удачной. В любом случае
СРОЧНО ПОМЕНЯЙТЕ ПАРОЛЬ

Признак 2: вам отвечают на письма, которых вы не отправляли.

Признак 3: непрочитанные письма вдруг стали прочитанными и вообще любые изменения, которые сделали НЕ ВЫ.