ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
В СОЦИАЛЬНЫХ СЕТЯХ

Логин

Иванов_

Пароль

s_3SD5q11_

ПАРОЛЬНАЯ ПОЛИТИКА

Хороший пароль = фраза из нескольких слов
+ спецсимволы + цифры

- Фраза на русском: Ваше политическое кредо? Всегда!
- Меняем все буквы «е» на цифры по порядку, буквы «с» на %: Ваш1 политич2%ко3 кр4до?В%5гда!
- Вбиваем английской раскладкой: Dfi1 gjkbnbx2%rj3 rh4lj?D%5ulf!
- Итоговый пароль без пробелов: Dfi1gjkbnbx2%rj3rh4lj?D%5ulf!



ПАРОЛЬНАЯ ПОЛИТИКА

- **Один аккаунт = один пароль**
- **Не используйте личные данные и их комбинации в пароле**
- **Не храните пароли на физических носителях и в открытом доступе**
- **Использование менеджеров паролей**

Логин

ivanovalex

Пароль

s_3SD5q11_

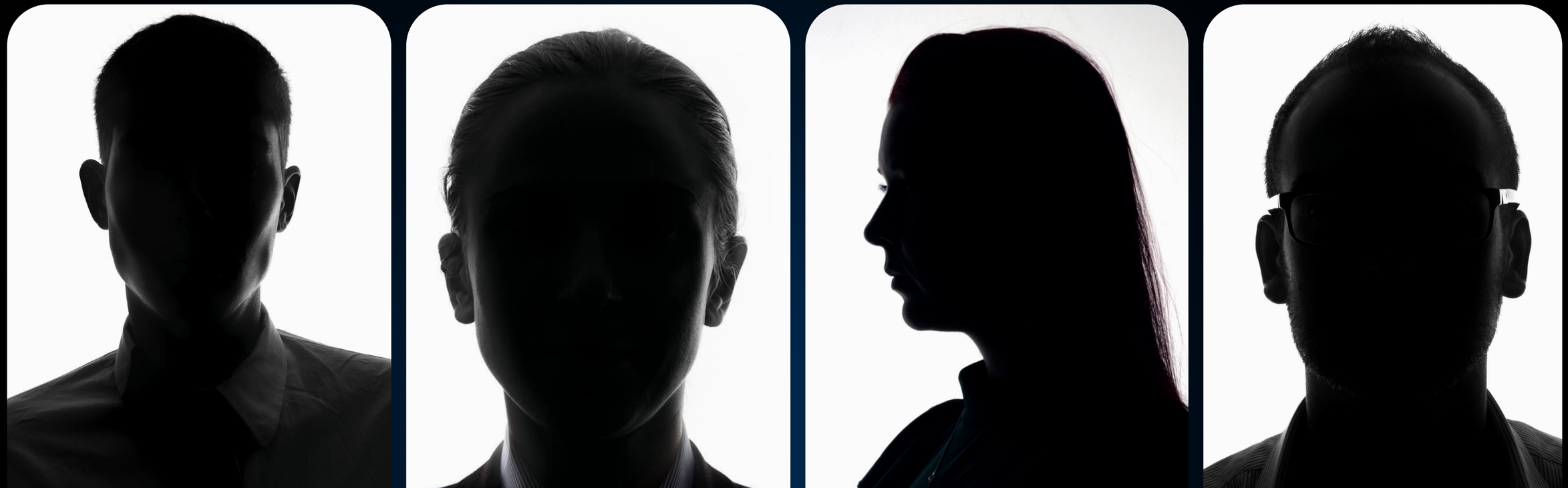
ФИШИНГ



- Не переходите по ссылке;
- Не копируйте адрес ссылки;
- Не открывайте и не скачивайте документы из письма (с телефона тоже нельзя);
- Не пересылайте письма коллегам;
- Не подгружайте картинки от незнакомых людей;
- Если вы сомневаетесь, кто отправил вам сообщение — по возможности свяжитесь с отправителем по другому виду связи.



БЕЗОПАСНОЕ ПРЕБЫВАНИЕ В СОЦИАЛЬНЫХ СЕТЯХ



1. ИСПОЛЬЗУЙТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

2. НЕ ПЕРЕДАВАЙТЕ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ В СОЦ.СЕТЯХ

3. НЕ ПУБЛИКУЙТЕ ДАННЫЕ, КОТОРЫЕ МОГУТ НАНЕСТИ РЕПУТАЦИОННЫЙ ВРЕД

4. ПРОВЕРЯЙТЕ ССЫЛКИ В АДРЕСНОЙ СТРОКЕ И В СООБЩЕНИЯХ

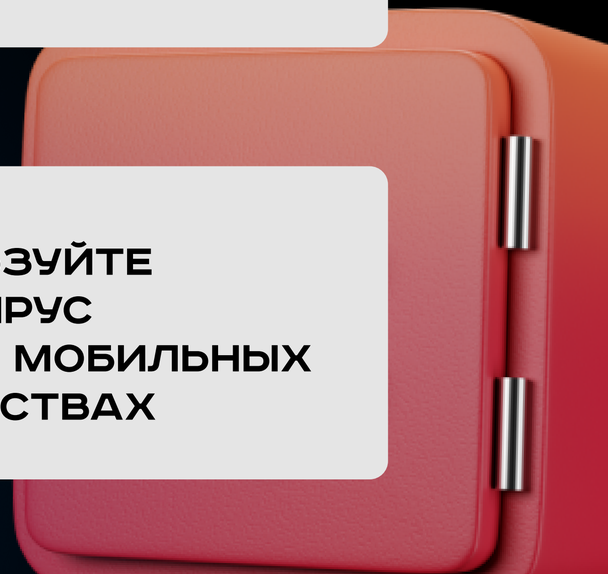
5. НЕ ПОЛЬЗУЙТЕСЬ АВТОСОХРАНЕНИЕМ ДАННЫХ В БРАУЗЕРЕ

6. ОБЯЗАТЕЛЬНО ВЫХОДИТЕ ИЗ АККАУНТА НА ЧУЖИХ УСТРОЙСТВАХ

7. НЕ ВВОДИТЕ ДАННЫЕ, ЕСЛИ НЕТ ПРОТОКОЛА HTTPS

8. НЕ УСТАНАВЛИВАЙТЕ РАСШИРЕНИЯ В БРАУЗЕРЕ БЕЗ КРАЙНЕЙ НЕОБХОДИМОСТИ

9. ИСПОЛЬЗУЙТЕ АНТИВИРУС НА ПК И МОБИЛЬНЫХ УСТРОЙСТВАХ



В МЕССЕНДЖЕРАХ

1. Используйте облачные пароли, pin-коды

2. Контролируйте активные сессии:
Telegram: Настройки – Устройства
WhatsApp: WhatsApp Web

3. Никому не сообщайте информацию из системных сообщений (проверочные коды, коды доступа).



ПСИХОЛОГИЧЕСКИЕ ПРИЕМЫ

ВИД АТАКИ:

1. Дефицит, недостаточность

Дефицит или возможность потерять что-либо, даже не материальное — сильный мотивирующий страх. Большая часть социальной инженерии основана именно на нем. При этом, предмет дефицита необязательно должен быть материальным.

ПРИМЕР ПИСЬМА:

Ваша учетная запись была или будет заблокирована/ отключена

Тактика запугивания пользователя эффективна: перед угрозой блокировки аккаунта пользователь теряет бдительность, переходит по ссылке в письме и вводит свои логин и пароль

ВИД АТАКИ:

2. Симпатия и доверие

Люди склонны идти навстречу тем, кто выражает свою симпатию, и тем, кому доверяют. Войдя в близкий круг общения часто играют на доверии.

ПРИМЕР ПИСЬМА:

Ваш друг оставил вам личное сообщение. перейдите по ссылке, чтобы прочитать

В подобных письмах злоумышленники скрываются за маской людей/ организаций, которые входят в ваш доверенный круг, чьи письма и сообщения не должны у вас вызвать подозрений.

ВИД АТАКИ:

3. Авторитет

Или навязывание своей воли другим. Злоумышленники часто используют фактический или предполагаемый авторитет для достижения своих целей. Например, образ представителя органов исполнительной власти или непосредственного руководства.

ПРИМЕР ПИСЬМА:

Письма от госслужб

Фишинговые письма приходят от имени различных госорганов с информацией о претензиях, которые возникли к пользователю со стороны государства. Чаще всего в письмах фигурируют МВД, ФНС и ФМС, а также организации системы здравоохранения

ВИД АТАКИ:

4. Социальная поддержка

Или навязывание своей воли другим. Злоумышленники часто используют фактический или предполагаемый авторитет для достижения своих целей. Например, образ представителя органов исполнительной власти или непосредственного руководства.

ПРИМЕР ПИСЬМА:

Возможные темы писем:

Фишинговые письма приходят от имени различных госорганов с информацией о претензиях, которые возникли к пользователю со стороны государства. Чаще всего в письмах фигурируют МВД, ФНС и ФМС, а также организации системы здравоохранения

СПАСИБО ЗА ВНИМАНИЕ!