памятка от StopPhish

КАК ХАКЕР МОЖЕТ ИСПОРТИТЬ ВАМ ЖИЗНЬ — И КАК ЕМУ ЭТОГО НЕ ДАТЬ

Антивирус — это хорошо. Но, к сожалению, самая уязвимая часть системы — это мы сами.

Один неосторожный клик — и уже утечка данных, шантаж, взлом банковского аккаунта или блокировка доступа к работе.

Вот краткая памятка, как не попасться и что делать, чтобы спокойно жить, работать и отдыхать.

Не открывайте файлы от незнакомцев
Риски: заражение устройства, удалённый доступ, шпионаж.
Что делать:
- Не открывайте вложения от незнакомцев, даже если «это накладная от ПЭК» или «акт от вашей бухгалтерии».
- Всегда проверяйте отправителя: podderzhka@sb3r.online — это не Сбер.
- Используйте антивирус с функцией анализа почтовых вложений.
- Лучше оповестить службу ИБ, чем потом объяснять, откуда утекли данные.

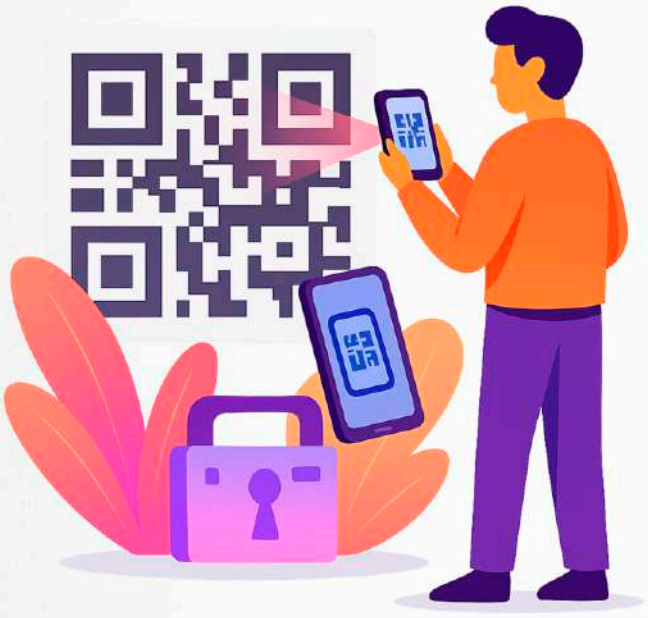
Камера — это глаз, который может смотреть на вас
Риски: хакеры могут получить удалённый доступ к камере через вредоносные программы, фальшивые приложения или уязвимости в системе.
Что делать:
- Заклейте камеру или установите шторку (есть красивые и недорогие).
- Проверьте доступы к камере в телефоне: соцсети, мессенджеры, приложения — всё по списку.
- Разрешайте доступ только нужным программам.

Потерянный телефон = открытый сейф

Риски: злоумышленник может получить доступ к банку, почте, мессенджерам, фотографиям и документам.

Что делать:

- Обязательно ставим пароль, Face ID или проверку отпечатка пальца для доступа в телефон.
- Включаем двухфакторную аутентификацию (двойную проверку доступа) в Telegram, ВКонтакте, Госуслугах и банках.
- Устанавливаем PIN-код на SIM-карту.
- Настраиваем удалённую блокировку и стирание данных (работает на Android или iOS).
- Подключаем резервное копирование в облако.



Осторожно с QR-кодами

Риски: мошенники могут наклеить поверх настоящего QR-кода свой — фальшивый. В результате вы попадёте на поддельный сайт, где у вас украдут логины, пароли или платёжные данные. Но даже без подмены они могут разместить вредоносный QR-код где угодно — например, в лифте вашего офиса или на стенде в подъезде.

Что делать:

- Сканируйте QR только с официальных источников: сайт банка, госоргана, магазина.
- После сканирования всегда смотрите адрес страницы — например, это должен быть sberbank.ru, а не sber-verify.ru.
- Дома используйте антивирус с защитой от фишинга — он предупредит об опасности.

Подозрительные устройства = ловушка

Что может быть: заражение вирусом, кража данных, шпионаж.

Что делать:

- Не используйте найденную флешку. Даже если она «лежала возле нашей переговорки».
- Не заряжайте телефон через найденные или бесплатные зарядки (например, в кафе или аэропортах).

Заблокированный счёт — неприятный сюрприз, особенно в поездках
Что теряется: деньги, время, нервы.
Что делать:
• Включите SMS или push-уведомления о входе в банк и транзакциях.
• Не сообщайте коды и логины, даже если звонят «из банка».
• Используйте отдельный номер телефона и почту для банков, если там много денег (номер может стоить 1 руб. в месяц, почта бесплатна).
• Заведите резервную карту и храните её отдельно, особенно когда путешествуете.

Финальные советы
1. Пароль от важных сервисов не должен быть 12345678. Для личных целей можно использовать бесплатные менеджеры паролей (например, Bitwarden или KeePass).
2. Включайте двухфакторную защиту — это реально работает.
3. Обновляйте Windows/MacOS и приложения. Обновления — это не каприз, а ваша защита.
4. Разделяйте рабочее и личное пространство. На рабочем компьютере не заходите в личные соц. сети, дома не используйте рабочую почту.

Помните:
Если что-то кажется подозрительным — значит, скорее всего, так оно и есть.
Опасность часто прячется в мелочах, которые мы склонны пропускать.
Но теперь – это не про вас.

С пожеланиями безопасности, StopPhish