ПАМЯТКА
ПО МОБИЛЬНОЙ БЕЗОПАСНОСТИ

1. Защита смартфона на случай его утери:

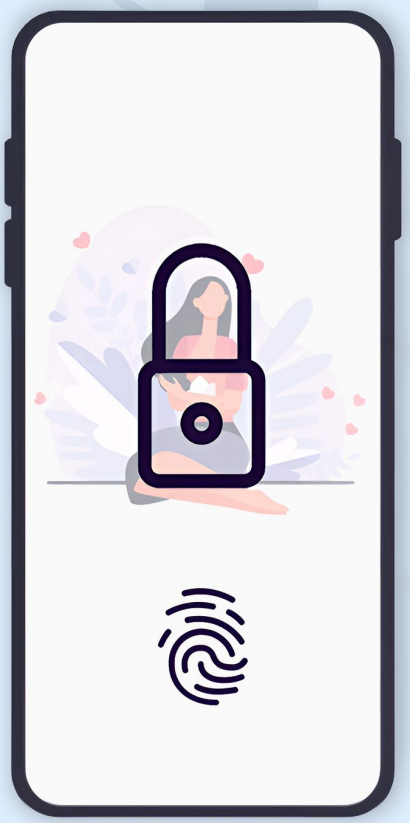
- Используйте пароль или биометрическую защиту для входа в телефон;

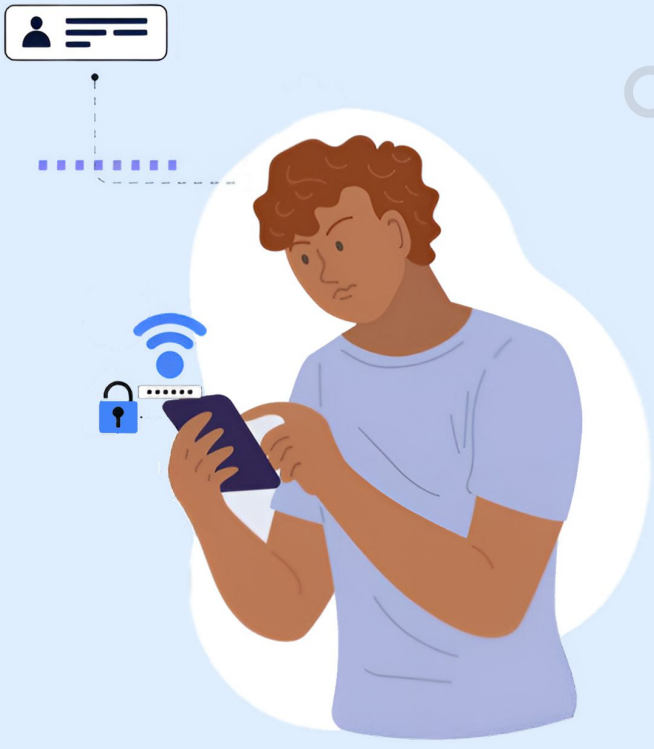
- Включите функцию «Найти устройство»;

- Установите PIN-код на SIM-карту. Так злоумышленник не сможет ею воспользоваться для входа в ваш банк и приложения;

- Отключите отображение SMS на заблокированном экране. Так никто не узнает одноразовый код, который отправляют некоторые сервисы для входа в личный кабинет;

- Удалите чувствительные данные с карты памяти. При утере телефона они будут доступны злоумышленнику.





2. Безопасность в сети:

- Избегайте использования публичных Wi-Fi сетей, если на каком-то сайте вам нужно ввести свой пароль. Он будет доступен владельцу Wi-Fi;

- Не отправляйте конфиденциальную информацию через бесплатный Wi-Fi.

3. Осторожность при звонках:

- Не сообщайте пароли и конфиденциальную информацию по телефону;

- Будьте бдительны при звонках от «служб безопасности» или «техподдержки». Перезванивайте по официальным номерам для проверки информации, которую вам сообщают;

- Если при разговоре вы слышите слово «деньги» или вам кто-то угрожает, даже если это родственник или руководитель, убедитесь, что это он вам звонит. Сверьте номер телефона или аккаунт в мессенджере с теми, что написаны на официальных сайтах или в ваших контактах. Может оказаться, что у звонящего «начальника» в Телеграм аккаунт написан как @pavei, а в ваших контактах руководитель записан как @pavel;

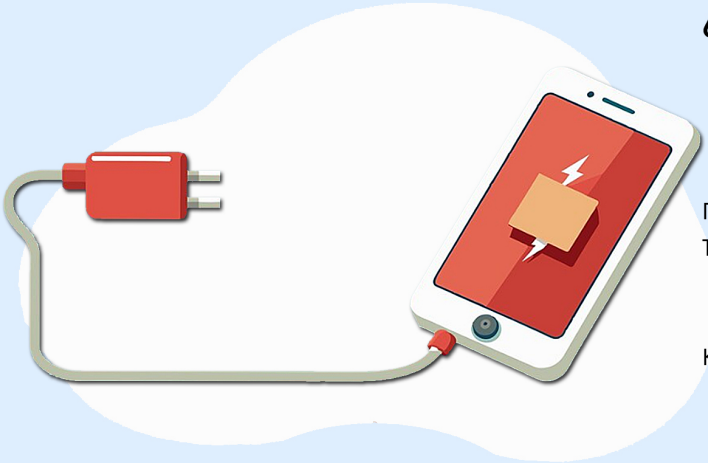
- Номер телефона при входящем звонке может быть подделан. Опять же, если разговор идет о деньгах или угрозе для вас, перезвоните по официальному номеру самостоятельно, а этот звонок завершите.

4. Приложения и QR-коды:

- Устанавливайте приложения только из официальных магазинов (App Store, Google Play);

- Проверяйте разрешения приложений;

- При сканировании QR-кодов в публичных местах проверяйте, не наклеен ли поверх него еще один QR. Относитесь к любому QR-коду, как и к любому сайту, на который вы можете попасть. Сайт мошенников может быть похож на официальный.



6. Физическая безопасность:

- Не оставляйте телефон без присмотра;

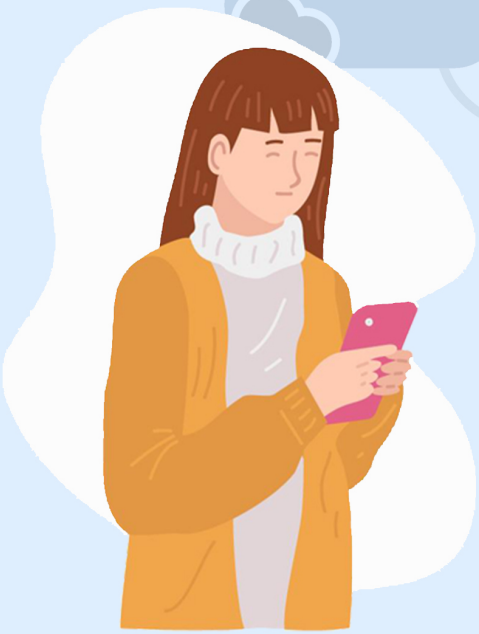
- Будьте осторожны при использовании публичных зарядных устройств. Используйте свой шнур для зарядки;

- Не подключайте телефон к незнакомым компьютерам.

7. Конфиденциальность:

- Не обсуждайте конфиденциальную рабочую информацию в общественных местах;

- Не копируйте рабочие документы на личное устройство и не отправляйте их на личную почту.



8. В случае потери или кражи телефона:

- Немедленно сообщите об этом в службу безопасности (если устройство корпоративное);

- Попытайтесь удаленно заблокировать устройство. Посмотрите в интернете, как это сделать;

- Смените пароли ко всем важным сайтам и службам.

С пожеланиями безопасности, StopPhish