Осторожно! Мошенники! Защитите свое устройство

Стационарный компьютер или ноутбук

- Регулярно обновляйте операционную систему и приложения на устройстве.
- Используйте актуальное лицензионное антивирусное ПО для защиты от вредоносных программ! Убедитесь, что антивирус автоматически ежедневно обновляется. Проводите регулярную полную проверку устройства на наличие вредоносных программ.
- Защитите учетную запись на вашем устройстве сложным, уникальным паролем. Не используйте один и тот же пароль для разных программ и доступов. Периодически меняйте ваши пароли на новые. Не сохраняйте ваши пароли в браузере (уберите галочку «сохранить»). Не записывайте и не храните логины, пароли или пины на стикерах или бумажных носителях в открытом доступе. Не сообщайте их никому, в том числе вашим работникам, системным администраторам, специалистам технической поддержке или любым другим лицам, которые могут представится работниками Fortebank или сотрудниками спецслужб.
- Установите двухфакторную аутентификацию на все важные системы, которые вы используете.
- Не используйте программное обеспечение для удаленного доступа (AnyDesk, TeamViewer и т.д.) на вашем устройстве.
- Старайтесь пользоваться интернет-банкингом на отдельном, специально подготовленном для этого устройстве. Ограничьте физический доступ к нему для третьих лиц.
- Блокируйте экран вашего устройства, даже если вы ненадолго покидаете рабочее место.
- Избегайте скачивания ненадежных файлов из сети интернет. Не устанавливайте взломанное или нелицензионное программное обеспечение на устройство.
- Используйте ограничения прав доступа, пользуйтесь учетной записью со стандартными правами. Избегайте использования учетной записи с административными привилегиями в повседневной работе. Это поможет предотвратить нежелательные изменения на вашем устройстве.
- Всегда проверяйте переносной носитель (флешку) антивирусной программой перед ее использованием. Скачанные с интернета файлы тоже проверяйте антивирусом перед их открытием.
- Включите встроенный межсетевой экран (брандмауэр) на вашем устройстве. Это поможет предотвратить несанкционированный сетевой доступ к вашему устройству.
- Обязательно храните резервную копию важной информации, чтобы в случае вирусной атаки или сбоя оборудования можно было восстановить данные.
- Не используйте устаревшую операционную систему, если на нее больше нет обновлений безопасности.

Мобильный смартфон или планшет

01 Регулярно обновляйте операционную систему и приложения на устройстве. Установите лицензионное антивирусное программное обеспечение и настройте автоматическое обновление сигнатур.

02 Используйте биометрические данные или сложный пароль/графический ключ для входа в устройство. Набирая пароль (или графический ключ) на смартфоне, убедитесь, что никто за вами не наблюдает.

03 Не передавайте устройство третьим лицам.

04 Установите двухфакторную аутентификацию на почту, мессенджеры, интернет-банкинги и прочие важные приложения.

05 Не записывайте пароли (уберите галочку «сохранять пароль») в приложениях на смартфоне.

06 Не принимайте подозрительные звонки в мессенджере, это могут быть мошенники. Удаляйте, не читая сообщения с подозрительных или иностранных номеров.

07 Проверяйте разрешения всех устанавливаемых приложений. Регулярно проверяйте список приложений. Удаляйте неиспользуемые.

08 Устанавливайте мобильные приложения только из официальных магазинов (Play Market, App Store), это упростить процедуру их регулярного обновления.

09 При скачивании приложения из официального магазина проверяйте производителя, рейтинг приложения и количество установок. Обращайте внимание на комментарии пользователей, установивших приложение ранее.

10 Перед продажей, утилизацией ПК, смартфона или планшета (корпоративного или личного) необходимо очистить жесткий память устройства, удаляя файлы без возможности восстановления или выполнить сброс до системных настроек.

С подробной информацией можете ознакомиться на сайте **forte.kz**, также можете **просканировать QR** для перехода на сайт