



**Как не стать жертвой
киберпреступников?**

Об актуальности защиты от киберпреступлений

В связи с ростом компьютерного хакерства кибербезопасность стала главной заботой среди ведущих направлений в сфере высоких технологий. Потребители, компании и даже государственные структуры вынуждены противостоять всё более наглým и изощрённым кибератакам. Многие из них включают в себя компьютерный саботаж и хищение информации, в том числе персональных данных.



Полезно знать

Что же делать простому пользователю ПК? Как не стать одним из жертв интернет-преступности? На помощь придут несколько дельных советов от профессионалов.

1. Тщательно контролируйте своё поведение в социальных сетях. Мошенники-виртуозы очень искусны в использовании личной информации, с помощью которой они с лёгкостью могут взломать коды безопасности, и получить доступ к другим учётным записям. За последние несколько лет этот способ кибератаки стал одним из самых распространённых.

2. Для сохранности ваших учётных записей ограничьте доступ к внутреннему кругу друзей и близких. Никогда не делитесь личной информацией с новыми интернет-друзьями. Старайтесь не афишировать данные, содержащие даты рождения, адреса электронной почты или имена домашних животных, которые могут использоваться как пароли. Вся эта информация может оказаться весьма полезной для профессионального хакера.



Полезно знать

3. Не используйте дебетовые карты онлайн. Несанкционированные платежи дебетовой карты изымаются непосредственно с вашего банковского счёта, и даже если вы немедленно сообщите о нарушении, на восстановление прежнего баланса потребуется не одна неделя. В случае с кредитной картой в аналогичной ситуации при оспаривании подозрительных оплат клиент имеет доступ к своим счетам. Оба вида карт имеют функции оповещения либо на электронную почту или в виде СМС-текста, что даёт возможность быстрого прерывания несанкционированных действий. Visa является лидером в области разработок защиты для своих кредитных карт.

4. Остерегайтесь сообщений подобного рода: «Внимание! Ваш аккаунт был взломан. Вы должны позвонить, чтобы подтвердить свой аккаунт. Отправьте нам сообщение, и мы перезвоним Вам».



Полезно знать

5. Не станьте жертвой Clickjacking. Этот вид атаки таит в себе гиперссылки под тем, что, на первый взгляд, выглядит как безобидный контент. Однако при нажатии ссылки открывается канал для вредоносных программ, которые могут вторгнуться в компьютер или передать вашу личную информацию.

6. Не будьте опрометчивы в использовании любого Wi-Fi соединения. Горячие точки Wi-Fi чаще всего небезопасны, так как не кодируют информацию, передаваемую в интернете. Более того, инструменты, которыми пользуются хакеры, позволяют им «заглянуть» через ваше плечо и выудить имена пользователей, пароли или другую информацию, предоставляющую доступ к финансовым счетам. Сотовая сеть в этом плане более безопасна.



Полезно знать

7. В сообщениях электронной почты и на веб-сайте, внимательно смотрите на URL-адреса, даже если они содержат имена авторитетных финансовых учреждений, с которыми вы имеете дело. Самый распространённый подвох – это комбинация имени законного веб-сайта и подделки. Эти адреса очень часто ведут на сайты-подражатели, которые под внешне законным видом скрывают принадлежность к хакерской деятельности. Иногда URL-адрес может оказаться подлинным, но когда вы нажимаете на ссылку, он переносит вас на другой сайт.

8. Никогда не кликайте на сообщения, присланные на электронную почту и предлагающие обновить персональные данные. В большинстве случаев такие запросы инициируются после того, как вы входите в свой аккаунт не через электронный адрес.

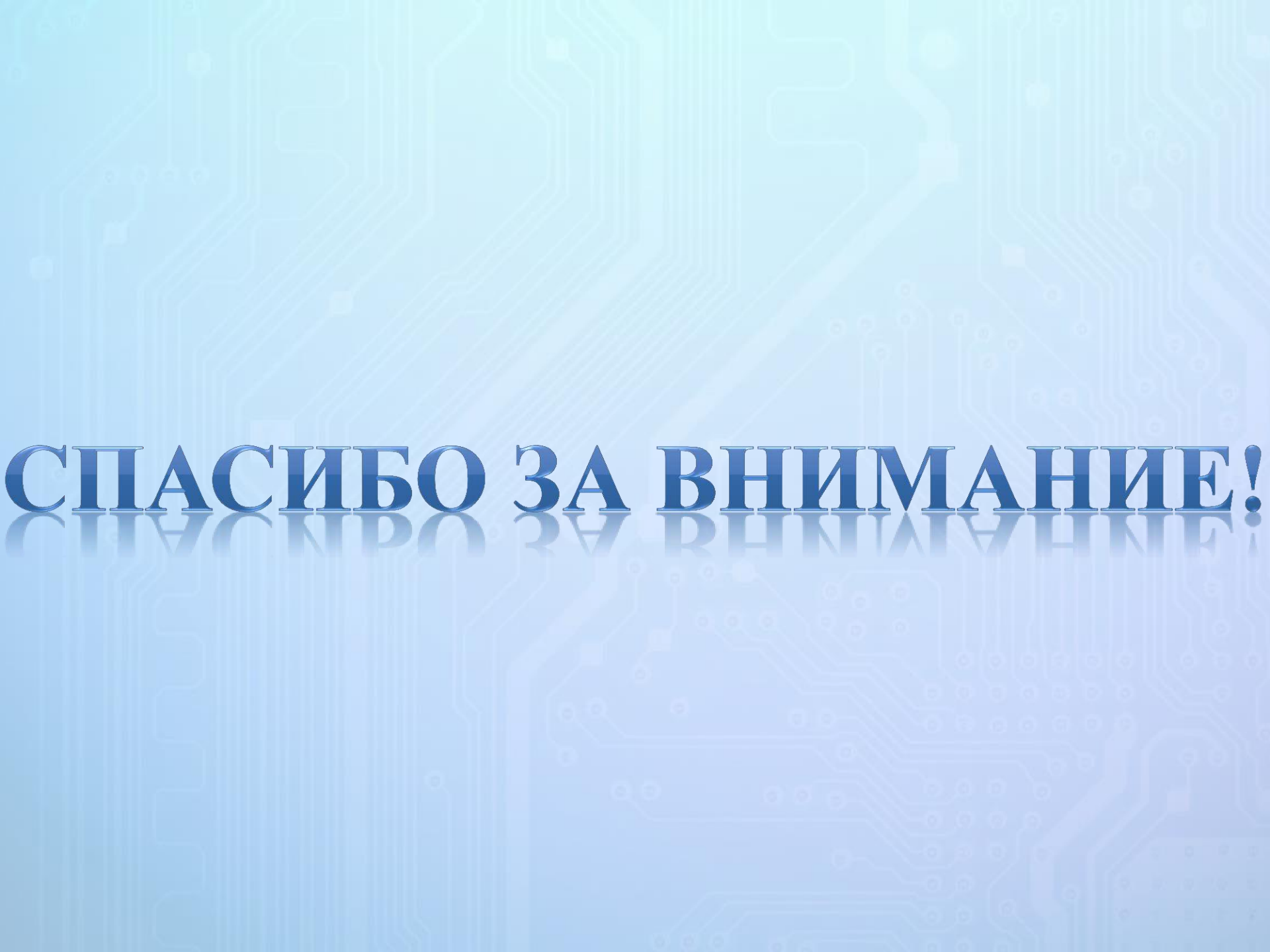


Полезно знать

9. Не используйте одинаковый пароль для разных учётных записей. Выбирайте для паролей необычные символы, цифры и пробелы. В качестве дополнительной меры предосторожности, заполните вопросы безопасности вымышленными, простыми для запоминания ответами, а не фактами, которые могли бы раскрыть ваши личные данные.

10. Установите на компьютер антивирусное и антишпионское программное обеспечение. Убедитесь, что эти программы работают и обновляются автоматически.





СПАСИБО ЗА ВНИМАНИЕ!