ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ

Прокуратура
Боровского района
разъясняет

ПОНЯТИЕ И ОСОБЕННОСТИ КИБЕРПРЕСТУПНОСТИ

Киберпреступление- это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Особенности киберпреступности:

- чрезвычайная скрытность деяний (применение механизмов анонимности и шифрования);
- трансграничность (преступник и жертва могут находиться на значительном расстоянии друг от друга);
-нестандартность способов совершения;
-автоматизированный режим.

ГРУППЫ КИБЕРПРЕСТУПЛЕНИЙ (по конвенции Совета Европы)

Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

Вторая группа- противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами).

Третья группа- противоправные деяния, связанные с содержанием данных или контентом.

Четвертая группа- нарушение авторских и смежных прав.

Пятая группа- кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность.

ОТВЕТСТВЕННОСТЬ ЗА СОВЕРШЕНИЕ КИБЕРПРЕСТУПЛЕНИЯ

Ответственность за киберпреступления в предусматривается главой 28 УК РФ и касается только компьютерных преступлений.
В зависимости от тяжести преступления и размера причиненного вреда статьи 272,273 и 274 УК РФ предполагают наказание в виде штрафа от 100 тыс. рублей, исправительных или принудительных работ от 6 месяцев до 5 лет, ограничения или лишения свободы до 7 л

СПОСОБЫ ЗАЩИТЫ ОТ КИБЕРПРЕСТУПЛЕНИЙ

1. Регулярно обновляйте программное обеспечение и операционную систему

Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

2. Установите антивирусное программное обеспечение и регулярно его обновляйте

Использование антивируса или комплексного решения для обеспечения интернет-безопасности- это правильный способ защитить вашу систему от атак. Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты.

3. Используйте сильные пароли

Используйте сильные пароли, которые трудно подобрать, и нигде их не записывайте. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сильный пароль.

СПОСОБЫ ЗАЩИТЫ ОТ КИБЕРПРЕСТУПЛЕНИЙ

4. Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, - это вредоносные ссылки в спамовых электронных письмах или других сообщения, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

5. Не предоставляйте личную информацию, не убедившись в безопасности канала передачи

Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

6. Свяжитесь напрямую с компанией, если вы получили подозрительный запрос

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.

СПОСОБЫ ЗАЩИТЫ ОТ КИБЕРПРЕСТУПЛЕНИЙ

7. Внимательно проверяйте адреса веб-сайтов, которые вы посещаете
Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Не переходите по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.
Если ваш продукт для обеспечения безопасности в Интернете включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

8. Внимательно просматривайте свои банковские выписки
Просматривайте внимательно свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.