Октябрь 2024 г.

Месячник кибер-безопасности

Защитите себя от кибермошенничества!

1. **Остерегайтесь фишинг-имейлов**
   Фишинг — это кража данных интернет-мошенниками с помощью поддельных имейлов. Киберпреступники отправляют электронные письма от имени других лиц с просьбой перейти по ссылке. Если имейл выглядит странным, проверьте имя отправителя и соответствует ли его электронная почта тому, за кого он себя выдает.

2. **Используйте многофакторную аутентификация (MFA)**
   MFA предоставляет дополнительный уровень безопасности. Обычно, это текстовое сообщение с кодом, который деактивируется после одноразового использования.

3. **Используйте сложный пароль**
   Не пользуйтесь одним и тем же паролем везде! Пароль должен содержать буквы, цифры и символы. Чем он длиннее, тем безопасней. Также полезны кодовые фразы.

4. **Обновляйте установленные программы**
   Это снижает риск заражения от программ, установленных хакерами, которые могут похитить вашу информацию или распространить вирусы на компьютере.

5. **Будьте осторожны и следите за безопасностью в социальных сетях**
   Личная информация, такая как день рождения, домашний адрес, местоположение, может быть использована для кражи личных данных или травли.

6. **Используйте безопасное подключение к сети Wi-Fi**
   Публичные сети не безопасны! Посторонние люди могут получить доступ к вашему имейлу или банковскому счету.

7. **Остерегайтесь мошенничества с использованием ИИ (AI)**
   Кибермошенники используют искусственный интеллект для создания реалистичных изображений, текстовых и голосовых сообщений и видео. Это затрудняет распознавание фишинга или других типов мошенничества. Будьте бдительны и осторожны (например, проверяйте источник, обращайте внимание на красные флажки ИИ и «артефакты», такие как эффект срочности, неестественные голоса или слегка искаженные изображения и т. д.), прежде чем отвечать на сообщения.

NYC Public Schools

diit