ФЕДЕРАЛЬНЫЙ ЭКОЛОГИЧЕСКИЙ ОПЕРАТОР РОСАТОМ

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Федеральная государственная информационная система учета и контроля за обращением с отходами I и II классов опасности.
Федеральный оператор по обращению с отходами I и II классов опасности.

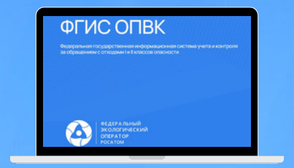
Основные угрозы информационной безопасности

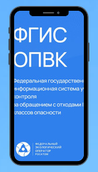
Фишинговые атаки

Цель фишинговых сообщений - заставить сотрудников организации раскрыть конфиденциальную информацию. Мошенники могут проявлять высокую осведомлённость о взаимоотношениях внутри компании. Например, они могут посылать электронные письма с адреса похожего на адрес кого-то из партнёров. В других случаях, наоборот, сотрудник дочерней (подрядной) организации может получить электронное письмо с мошеннической ссылкой.

Социальная инженерия

Атаки методом социальной инженерии заключаются в том, чтобы обманом заставить пострадавшего разгласить конфиденциальную информацию. Чат-боты стали важным инструментом онлайн-продвижения в интернете. Сегодня хакеры научились создавать поддельные чат-боты, чтобы заставить покупателей и партнёров раскрыть конфиденциальную информацию.





Кража паролей

Этот тип атаки также носит массовый характер. Он часто встречается когда злоумышленники могут подсмотреть и украсть пароль при его вводе или неправильном хранении. Краже подвержены также устройства, которые записывают ввод паролей. Нередки случаи установки фишинговых хот - спотов Wi-Fi, когда мошенники подделывают оригинальную точку доступа Wi-Fi, задавая общее имя.

Троянские атаки

Трояны - это приложения, которые выдают себя за то, чем на самом деле не являются. Они маскируются под законные приложения. Основная цель троянов - создать возможность загрузки вирусов на устройство пользователя и далее осуществить загрузку в иные информационные системы (например - ФГИС ОПВК).

Черви

Такие вредоносные программы способны распространяться и размножаться после проникновения на устройство пользователя и далее в иные информационные системы (например - ФГИС ОПВК).

Как себя обезопасить?

Проверяйте источник

В условиях современной цифровой реальности злоумышленники используют все существующие методы социальной инженерии для того, чтобы вынудить пользователя совершить фишинговое действие, которое окажется для него вредоносным, а для мошенников – выгодным.
Важно! Фишинговые ссылки могут поступать через все каналы: социальные сети, личный и рабочий e-mail, мессенджеры, SMS, а также чаты на сайтах знакомств и подобных ресурсах.

Надежный аккаунт

Используйте уникальный и сложный пароль! Сложный пароль состоит из минимум восьми символов, включая большие и маленькие буквы, цифры и специальные символы. Пример такого пароля: «oPQ0nz$Hx4%!».Не стоит пренебрегать требованиями к паролю, поскольку это одна из самых важных преград перед возможными мошенниками. Не используйте пароль от других служб и соцсетей. По возможности повысьте безопасность аккаунта путем настройки дополнительных мер защиты (включите двухэтапную проверку входа, вход по электронной подписи, оповещения о входе в ваш аккаунт и т.п.)

Фейковые сайты

Проверяйте доменное имя сайта! Распознать фейковый сайт можно только по доменному имени, оно очень схоже с официальным адресом сайта, но всё же, при должном внимании можно заметить расхождения (дополнительные буквы, символы, цифры). Дизайн и наполнение сайта практически повторяет настоящий. При авторизации на данном сайте, мошенники извлекут Ваши учетные данные.

Антивирусные программы

Антивирусная программа (средство антивирусной защиты, средство обнаружения вредоносных программ)— специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.