ФИШИНГ ИЛИ КРАЖА ЛИЧНЫХ ДАННЫХ

ОБЫЧНОЙ КРАЖЕЙ ДЕНЕГ И ДОКУМЕНТОВ СЕГОДНЯ УЖЕ НИКОГО НЕ УДИВИШЬ, НО С РАЗВИТИЕМ ИНТЕРНЕТ-ТЕХНОЛОГИЙ ЗЛОУМЫШЛЕННИКИ ПЕРЕМЕСТИЛИСЬ В ИНТЕРНЕТ, И ПРОДОЛЖАЮТ ЗАНИМАТЬСЯ "ЛЮБИМЫМ" ДЕЛОМ.

ТАК ПОЯВИЛАСЬ НОВАЯ УГРОЗА: ИНТЕРНЕТ-МОШЕННИЧЕСТВА ИЛИ ФИШИНГ, ГЛАВНАЯ ЦЕЛЬ КОТОРОГО СОСТОИТ В ПОЛУЧЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ - ЛОГИНОВ И ПАРОЛЕЙ. НА АНГЛИЙСКОМ ЯЗЫКЕ PHISHING ЧИТАЕТСЯ КАК ФИШИНГ (ОТ FISHING - РЫБНАЯ ЛОВЛЯ, PASSWORD - ПАРОЛЬ).

ОСНОВНЫЕ СОВЕТЫ ПО БОРЬБЕ С ФИШИНГОМ:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.