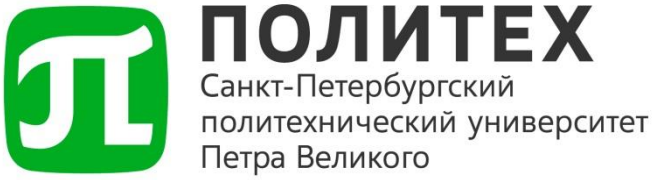
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»



РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОТ ФИШИНГОВЫХ АТАК

Санкт-Петербург

2025 г.

Типовые схемы фишинговых атак на работников и обучающихся

Самозапрет на кредит

Злоумышленник осуществляет звонок по сотовой связи или с использованием одного из мессенджеров, представляясь сотрудником портала «Госуслуги», и сообщает о технической ошибке при установлении самозапрета на кредит. Далее для исправления заявления злоумышленник просит перейти по направленной в мессенджере ссылке. При переходе по указанной ссылке пользователь попадает на веб-сайт, имитирующий портал «Госуслуги», и вводит свои аутентификационные данные. Далее с использованием указанных аутентификационных данных злоумышленник может получить доступ к личному кабинету на настоящем портале «Госуслуги».

Смерть близкого человека

Злоумышленник с использованием одного из мессенджеров отправляет сообщение о смерти близкого человека, прикрепляя вирусный файл под видом фотографии «умершего». Находясь в состоянии стресса, пользователь может открыть прикрепленный файл. В результате запуска вредоносного файла злоумышленник может получить доступ к личным данным пользователя, хранящимся на устройстве, а также далее по цепочке отправить аналогичное сообщение всем контактам пользователя.

Скачай приложение для защиты

Злоумышленник осуществляет звонок по сотовой связи или с использованием одного из мессенджеров, представляясь сотрудником службы безопасности Центробанка РФ, и настоятельно просит скачать приложение, которое якобы предотвратит кражу денег во время звонка. Злоумышленник пытается вызвать панику, убеждая, что прямо сейчас производятся противоправные действия, и необходимо срочно принять меры. В ряде случаев фишинговое приложение злоумышленникам удается разместить в официальном магазине приложений Google Play. После установке приложения злоумышленник перехватывает всю информацию с устройства (в т.ч. звонки и СМС-сообщения). Далее злоумышленник может получить доступ к личному кабинету на портале «Госуслуги» и приложениям банков.

Звонок от помощника судьи

Злоумышленник осуществляет звонок по сотовой связи или с использованием одного из мессенджеров, представляясь сотрудником суда, и сообщает о рассмотрении судебного дела. Далее злоумышленник информирует о назначении судебного заседания и просит подтвердить явку или согласие на рассмотрение дела без участия гражданина. Для подтверждения решения злоумышленник требует назвать код, содержащийся в полученном СМС-сообщении. На самом деле этот код – подтверждение смены пароля от личного кабинета на портале «Госуслуги». Далее злоумышленник может получить доступ к личному кабинету на портале «Госуслуги».

Проверка телефонной линии

Злоумышленник осуществляет звонок по сотовой связи или с использованием одного из мессенджеров, представляясь сотрудником оператора сотовой связи, и сообщает о необходимости проверить телефонную линию. Злоумышленник просит нажать на телефоне

комбинацию клавиш #90 или #09. Если ввести данную комбинацию, то злоумышленник получит полный доступ к SIM–карте. Получив полный контроль над SIM–картой, злоумышленник может снять средства с баланса номера телефона, войти в мессенджеры, личный кабинет на портале «Госуслуги» и банковские приложения для оформления кредитов и кражи денег.

Рекомендации по защите от фишинговых атак

Соблюдайте бдительность, не отвечайте на подобные звонки и сообщения, не переводите деньги, не сообщайте злоумышленникам персональные данные, логины и пароли к информационным системам, а также не передавайте сведения, составляющие конфиденциальную информацию.

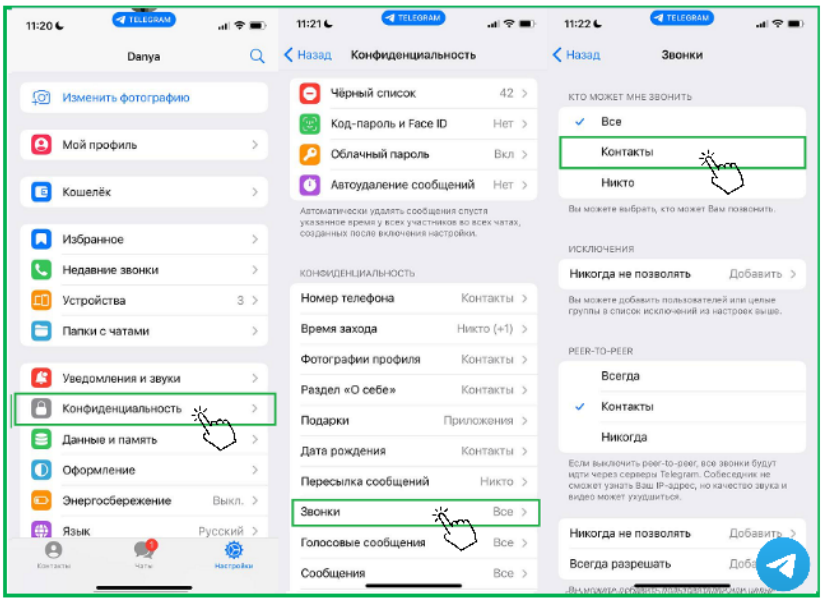
Не открывайте файлы от незнакомых людей и не скачивайте неизвестные приложения.

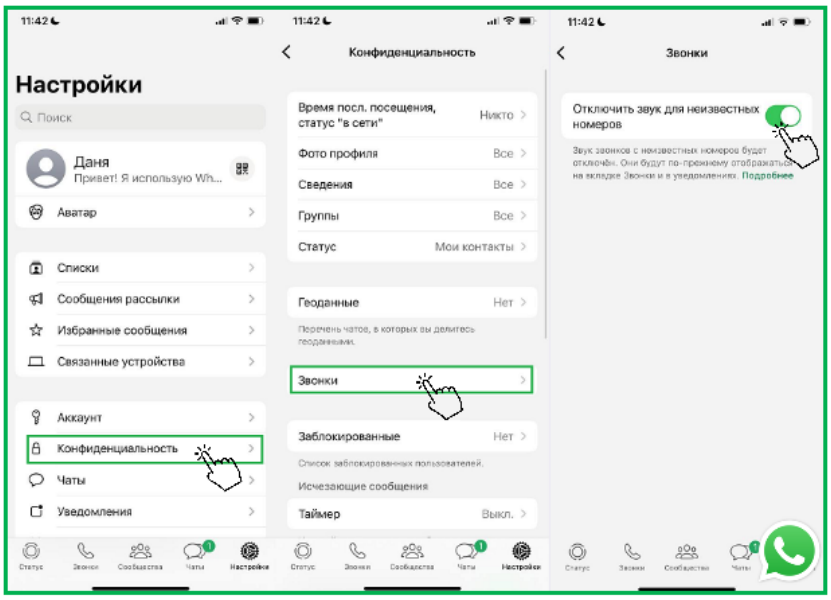
Установите на телефон определитель номера (например, Kaspersky Who Calls или бесплатный определитель номера Яндекса).

Запретите в мессенджерах Telegram и WhatsApp получение звонков с незнакомых номеров:

- откройте приложение Telegram и перейдите в раздел «Настройки». В меню выберите раздел «Конфиденциальность» → «Звонки». В разделе «Кто может мне звонить» выберите «Контакты»;

- откройте приложение WhatsApp и перейдите в раздел «Настройки». В меню выберите раздел «Конфиденциальность» → «Звонки». Включите опцию «Отключить звук для неизвестных номеров».





При использовании мессенджеров настройте двухфакторную аутентификацию. Если злоумышленники получили доступ к Вашей учетной записи в одном из мессенджеров, можно попытаться ограничить их доступ. Для этого в мессенджере зайдите в меню «Настройки» → «Активные сессии» и нажмите на кнопку «Завершить все другие сеансы».

При получении подозрительных звонков и сообщений следует обратиться в Службу поддержки пользователей по телефону +7-(812)-775-05-10 или электронной почте support@spbstu.ru.