КИБЕРПРЕСТУПНОСТЬ

ОСНОВНЫЕ АСПЕКТЫ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПЛЕНИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Стремительное развитие цифровых технологий, резкое увеличение предоставляемых населению числа электронных услуг, а также отсутствие у граждан базовых навыков защиты личной информации в интернете привели к устойчивому росту количества киберпреступлений. Так, если в 2015 году их было совершено 2,4 тысячи, то в 2020 – уже 25,5 тысячи. Технический прогресс способствует тому, что аналогичные негативные тенденции продолжают развиваться. К сожалению, сегодня большинство граждан недостаточно информированы о методике действий кибермошенников, формально относятся к защите собственной информации, персональных данных, а, следовательно – имущества.

Что же такое фишинг и вишинг, как защитить свою банковскую карту, какие правила безопасного поведения в соцсетях и месенжерах должен знать каждый.

ФИШИНГ – (*от англ. phishing – выуживание*) – это вид интернет-мошенничества, который заключается в краже конфиденциальных данных пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Чаще всего фишинг представляет собой массовые рассылки писем и уведомлений от имени известных брендов, банков, платежных систем, почтовых сервисов, социальных сетей. Такие письма, как правило, содержат логотип, сообщение и прямую ссылку на сайт, внешне неотличимый от настоящего. По ссылке требуется перейти на сайт «сервиса» и под различными предлогами ввести конфиденциальные данные в соответствующие формы. В результате мошенники получают доступ к аккаунтам и банковским счетам пользователей.

ВИШИНГ – способ мошенничества с помощью телефона, когда мошенник под различным предлогом пытается выманить персональную информацию жертвы для последующего хищения денег с ее банковского счета.

В Республики Беларусь уже зафиксированы случаи совершения хищения денежных средств со счетов белорусов мошенниками, которые под видом «лжебанкиров» звонят на телефоны белорусов и выведывают конфиденциальную информацию.

Однако киберпреступники регулярно видоизменяют свои преступные схемы. В Республике Беларусь зафиксирована обновленная схема вишинга, жертвами которой уже стали жители Гомельской и Могилевской областей. Мошенники для введения жертв в заблуждение действовали от имени якобы сотрудников правоохранительных органов.

Сотрудники Министерства внутренних дел Республики Беларусь предупреждают!

Вишинг-атаки совершаются методом социального инжиниринга. Нападающий создаёт критическую ситуацию, позволяющую эксплуатировать человеческие чувства, и убеждает жертву раскрыть ценную информацию. Мошенники используют фактор неожиданности и создают для жертвы максимально неудобные условия при нехватке времени на анализ происходящего. Обычно их интересует номер банковской платежной карты, логин и пароль от кабинета.

Чтобы не стать жертвой киберпреступника, необходимо соблюдать следующие правила цифровой безопасности:

- необходимо помнить, что по телефону собеседник может представляться кем угодно. Поэтому будьте бдительны и никогда не сообщайте незнакомым людям конфиденциальные данные. Кем бы они ни представлялись, как бы убедительно ни звучали их просьбы. Запомните: сотрудники банков или госучреждений никогда не будут у вас спрашивать данные, к которым у них и без того есть доступ!

- не устанавливайте на свой мобильный телефон какие-либо программы по просьбе неизвестных вам людей, и не предоставляйте им доступ к ранее установленным.

- обезопасьте свой основной банковский счет! Для совершения онлайн-платежей откройте в том же банке другой счет, который сможете пополнять при необходимости. И если даже этот счет будет скомпрометирован, ваш основной останется в безопасности.