

## **1. Виды мошенничества:** кардинг, киберпреступность, хакинг, скимминг, фишинг.

В настоящее время кардинг является самым популярным видом мошенничества. Социальные сети предлагают прикреплять карты к аккаунту. Одно неловкое движение пальцем может снять определённую сумму денег с карты пользователя на ненужную ему услугу.

### **2. Кардинг:**

Мошенничество с платежными картами, **кардинг** (от англ. carding) — вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтвержденная её держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы коннекта (процесс и результат установления связи между удалёнными компьютерами с помощью модема или другими способами), «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространённым методом похищения номеров платежных карт на сегодня является фишинг, например —зеркало сайта социальной сети, через которое и происходит похищение реквизитов платежных карт.

### **3. Фишинг:**

**Фйшинг** (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Немаловажную популярность имеет киберпреступность. Мошенники так и норовят узнать персональные данные о пользователе. Где же найти много интересного о человеке? Конечно же в социальной сети. Сам пользователь социальной сети собственноручно передаёт свои персональные данные мошенником, указывая всю информацию о себе в аккаунте.

### **4. Киберпреступность:**

**Киберпреступность** – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также

распространение противоправной информации (клеветы, порнографических материалов) через Интернет.

Киберпреступлениями также считаются интернет-аукционы в социальных сетях, в которых сами продавцы делают ставки для того, чтобы поднять цену выставленного на аукцион товара.

#### **5. «Чикиниться», «хэштег»:**

Подробнее опишу функцию "чкиниться" - отметить. Человек, посетив определённое место, чаще крутое заведение, даёт понять мошеннику, что он живёт в достатке, что его нет в данный момент дома либо на работе.

Функция "хэштег" позволяет находить фотографии, видео либо посты на определённую тему. #море, #клуб. Как же попадали пользователи в руки кураторов игры "Синий кит", "F57", "Розовая мартышка", "Оранжевый попугай"? Правильно, они указывали в своём профиле хэштег #Синийкит, #тихийдом, #420, #хочувигру, #f57 и т.д. Куратор отправляет ссылку, по которой переходит ребёнок, тем самым передавая свои данные в руки мошенника.

Все это позволяет мошенникам получать информацию о пользователе не прилагая усилий.

А как пользоваться выше перечисленной полученной информацией, мошенник распоряжается сам. Есть возможность записать на другого человека левую фирму, внушить пользователю, что его или родственников могут убить, если тот не передаст определённую сумму либо не выполнит определённые задания, примером является "Синий кит", "Розовый пони" и т.д.

#### **6. Хакинг:**

**Хакинг** – внесение изменений в программном обеспечении, для достижения определенных целей, отличающихся от целей создателей программ, очень часто изменения являются вредоносными. Человека, занимающегося хакингом, называют хакером.

#### **7. Скимминг:**

**Скимминг** – вид мошенничества с банковскими картами, который предусматривает использование различных устройств типа – скиммер. С помощью таких устройств мошенники считывают информацию, содержащуюся на магнитной полосе карты.

Сохранение карт в социальных сетях можно отнести к скиммингу, так как на сайте указываются данные карты с лицевой и обратной стороны. Имея на устройстве вредоносное ПО (Android.PWS.Vk.3), которое может украсть пароль и логин пользователя, можно передать доступ к аккаунту с прикрепленной картой мошенникам.

***Нельзя указывать персональные данные, номера карт, телефонов и другую информацию в аккаунте социальной сети, так как вы можете столкнуться с выше изложенными видами мошенничества.***