Родителям о кибермошенничестве

ИНТЕРНЕТ-РИСКИ:

- ОПАСНЫЙ КОНТЕНТ
- КИБЕРБУЛЛИНГ
- ВСТРЕЧИ С ОНЛАЙН-НЕЗНАКОМЦАМИ
- **КИБЕРМОШЕННИЧЕСТВО**
- ВИРУСЫ
- ИНТЕРНЕТ ЗАВИСИМОСТЬ

Кибермошенничество

- Кибермошенничество – один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения
личной информации пользователя (номера банковских счетов,
паспортные данные, коды, пароли и др.).

Виды кибермошенничества, которых надо остерегаться

- Вы проверяете ваш банковский счет, и оказывается, что деньги куда-то исчезли. В банке вам ничего не могут внятно объяснить и вообще говорят, что все с вашим счетом в порядке …

Виды кибермошенничества

- Скорее всего, вы стали жертвой кибермошенников. Именно с платежными карточками и системами интернет-банкинга они работают чаще всего. Сейчас хакеры активизировались также в сфере он-лайн платежей: разворовывают средства с использованием мобильных бот-сетей, заражают вирусами смартфоны и планшеты, атакуют POS-терминалы.

- Существует много способов сделать это: от простого «подглядывания» до «высокохудожественного» фишинга.

Скимминг

- На банкоматах или POS-терминалах в торговых точках устанавливают специальные устройства, которые считывают данные с ваших карточек. Это и называется **скимминг** (англ. — Быстро просматривать).
- И вот вы вводите свою карточку, а закреплена рядом с банкоматом видеокамера узнает ваш PIN-код и передает его преступникам. Далее мошенники изготавливают ее дубликат, который, в комплекте с PIN-кодом, позволяет снять деньги с вашего счета.

Как обойти?

- Для защиты от скимминга банкиры рекомендуют использовать карточки только в тех местах, которые заслуживают доверия и охраняются. Потому что камеры вы можете просто не заметить.

Вирусы, работающие с системами он-лайн-банкинга

- Сейчас этот вид мошенничества уже стал самым распространенным. На ваш компьютер определенным образом попадает вредоносное программное обеспечение. И когда вы пытаетесь зайти в свой аккаунт в платежной системе, вводя одноразовые пароли — эта программа выдает вам сообщение о якобы устаревший пароль. И каждый следующий код тоже оказывается «устаревшим».

Вирусы, работающие с системами он-лайн-банкинга

- А в это время вредоносное ПО именно входит в вашего банковского профиля, используя ваши же пароли и получает полный доступ к системе вашего онлайн- банкинга.

Как обойти?

- Для защиты эксперты рекомендуют постоянно контролировать карточный счет, подключить к нему смс-банкинг, не оставлять персональные данные о себе и своей карточку на интернет- сайтах, регулярно обновлять антивирусную защиту, особенно с функцией безопасных платежей.
- Кроме того, банкиры советуют открыть отдельную платежную карту для расчетов в Интернете, во многих финучреждений есть для этого специальный продукт — виртуальная карта.

Программа-вымогатель

- Вирус может зашифровать файлы на вашем компьютере, заблокировать ваш доступ к нему, или к любой онлайн-системы, в которой вы зарегистрированы. На экране вы будете видеть только картинку-блокер, и требование заплатить выкуп для того, чтобы расшифровать или разблокировать систему.

Например, такие:

- «Отправьте SMS на короткий номер»
  «Переведите деньги на мобильный счет»
  «Расплатитесь биткоинами (электронными деньгами)»

Как обойти подобную ловушку?

- Чтобы не «подхватить» вредоносное ПО такого вида, рекомендуется никогда не кликать по ссылкам на сайты банков или других финорганизаций. Надо вводить адрес **вручную**, иначе есть риск, что вы можете попасть на поддельную страницу, которая выглядит точно так же, как и оригинал.

Фишинг

- Если вам на электронную почту, телефон или другие веб-сервисы приходят сообщения от имени банка, будьте внимательны!
- Вам могут подсунуть поддельную интернет-страницу банка. На ней, с помощью различных психологических приемов, побудить вас ввести свои логин и другие ваши конфиденциальные данные, например номер карты, CVV-значение (три цифры на обратной стороне карты), ПИН- код. Имея их, кибермошенники получат доступ к аккаунтам и банковским счетам. Этот вид интернет-мошенничества называется фишинг (англ. Phishing, от fishing — рыбалка).

Как обойти ловушку?

- Фишинг — одна из разновидностей социальной инженерии, основанный на том, что вы не знаете основ сетевой безопасности. Следует знать простой факт: сервис не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее.
- Для защиты от фишинга производители основных интернет-браузеров договорились о том, что они будут применять одинаковые способы информирования пользователей о том, что человек попал на подозрительный сайт, который может принадлежать мошенникам.
- Новые версии браузеров уже имеют возможность, которая называется «антифишинг».

Кто будет платить за кибермошенников?

- Банкиры говорят, что в результате деятельности кибермошенников основные потери несут не банки, а клиенты, так как в большинстве случаев потери средств виноваты именно они. Причиной потерь может быть как незнание опасностями, так и то, что очень часто люди отказываются от всех дополнительных мер защиты для безопасной работы с системами клиент-банк.

Кто будет платить за кибермошенников?

- Банки же, в основном, подвергаются репутационные риски, которые возникают в основном не за низкого уровня защиты систем банка, а из-за нежелания клиента защищаться. **А незнание опасностей, невнимательность и халатное отношение к собственным средствам не освобождает владельца банковской карты от ответственности за последствия.**

Будьте бдительны!