ОСНОВЫ ФИНАНСОВОЙ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ – КАК ЗАЩИТИТЬ СВОИ ФИНАНСЫ

Борозенец Виктор,
к.э.н., доцент кафедры финансов и кредита СКФУ
Куницына Наталья,
д.э.н, профессор, заведующий кафедрой финансов и кредита СКФУ,
региональный координатор ФСМЦ по финансовой грамотности

Дружи с финансами

СКФУ СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

Угрозы потерять свои деньги в сети можно условно разделить на две группы:

1. Проникновение вирусных программ в компьютер или смартфон с целью их повреждения или сбора информации, в частности, паролей от различных аккаунтов.

2. Осуществление различных мошеннических действий в сети Интернет.

Рекомендации по первой группе угроз - лицензионное антивирусное ПО, предварительная проверка устанавливаемых программ, использование нескольких уровней защиты, дополнительных паролей.

Дополнительные способы защиты от вредоносных программ:

- регулярное резервирование данных;
- регулярное обновление.

Осуществление различных мошеннических действий в сети Интернет

- технологическое мошенничество – использование сайтов-двойников, проникновение к аккаунтам (фишинг) и другие способы;
- действия, связанные с хищением чужого имущества или приобретение права на чужое имущество путём обмана;
- воздействие на поведенческие стереотипы граждан.

Как распознать фишинг

- Убедитесь, что адрес сайта (URL) в адресной строке браузера набран корректно.
- Убедитесь, что URL является безопасным и начинается с “https”.
- Обратите внимание на любые расхождения с тем, как обычно выглядит интересующая вас веб-страница.
- Будьте внимательны по отношению к любой необычной активности на вашем банковском счёте.

Хищение чужого имущества путём обмана в Интернете

Основные формы:

- объявления о продажах товаров или оказания услуг;
- объявления о покупке товаров и услуг;
- объявления о предоставлении кредита.

Появившийся общий признак финансовой опасности

Коронавирус COVID-19.
«Бизнес» на панике и в условиях психологической усталости - online.

Продажа товаров для защиты от вируса через Интернет по завышенным ценам или ненадлежащего качества.

Предложение товаров для лечения вируса, при отсутствии таковых на рынке или научно не доказанной эффективности и безопасности.

Предложения по осуществлению различных «выгодных» финансовых сделок в условиях высокой волатильности рубля.

Сбор денег на помощь тем, кто заразился коронавирусом.

Информация о правонарушениях, связанных с мошенничеством, по итогам 1 квартала 2020 года

63,1% от общего числа зарегистрированных мошенничеств составляют совершенные с использованием **телекоммуникационных сетей**. При этом рост по сравнению с 1 кварталом 2019 года составил **40,3%**.

Основные преступления, совершенные с использованием сети **Интернет,** это объявления о продажах, о приёме на работу, о сдаче жилья в аренду.

Объявления размещались на сайтах: «Авито.ру», «ВКонтакте», «Инстаграм», «Одноклассники.ру», «Юла» и других сайтах.

Анализ раскрытых преступлений показал, что практически все преступления совершаются ***лицами***, находящимися ***за пределами*** определенного региона.

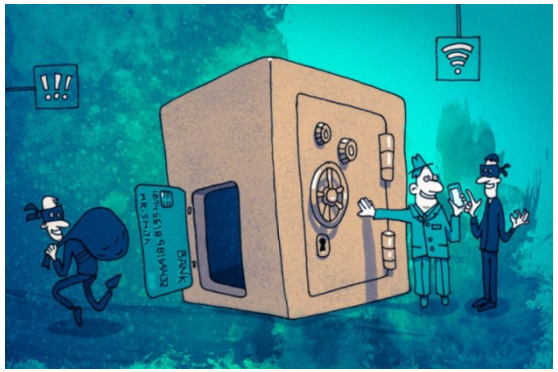
Количество IT-преступлений в стране выросло на **83,9%**, по сравнению с аналогичным периодом прошлого года

Основные общие признаки финансовой опасности (1)

- Вознаграждение существенно превышает деловую практику по данному типу сделок.
- Использование технологий «социальной инженерии» и манипулирование интересами, такими как жадность, желание быстро разбогатеть, зависть.

Основные общие признаки финансовой опасности (2)

- Предложение решить все финансовые проблемы в короткий срок.
- Необходимость первоначальных выплат.
- Анонимность контрагента.
- Необходимость быстрого принятия сложного финансового решения.



Поведенческие стереотипы потерпевших от финансовых мошенничеств (1)

- Нацеленность на высокий гарантированный доход, несоразмерный объёму инвестиций.
- Неадекватно высокий уровень доверия к контрагентам, граничащий с наивностью.
- Отсутствие критического взгляда на фактическое состояние ситуации.
- Нарушение регламента пользования финансовыми инструментами.

Поведенческие стереотипы потерпевших от финансовых мошенничеств (2)

•Невнимательность при осуществлении транзакций с использованием программных продуктов.

•Низкая финансовая грамотность.

•Нежелание погружаться в детали сделки или читать условия договора в полном объёме.

•Технологическая отсталость в условиях современных финансовых взаимодействий.

•Высокая готовность к риску, зачастую на грани «русской рулетки».

Правила интернет безопасности (1)

1. Основное правило – необходимо воспринимать Интернет как систему, функционирующую по своим правилам, и эти правила необходимо соблюдать.

2. Думайте о защите своего Интернет-устройства.

3. Переводите деньги только друзьям, с которыми есть не только контакт в сети.

4. Покупайте только у продавцов, которым есть основания верить.

5. Платите в сети только специальной банковской картой. Не кладите на нее большую сумму денег.

Правила интернет безопасности (2)

6. Старайтесь не открывать сайты платёжных систем по ссылке (например, в письмах).

7. Никогда и никому не сообщайте ваши пароли.

8. Не принимайте предложений об участии в различных проектах, если это требует уплаты взноса.

9. Выходя в Интернет с общественного компьютера или подключая своё оборудование к публичным сетям (например, в кафе), не совершайте онлайн-покупки, не заходите на сайты под своим логином.

10. Не соглашайтесь на просьбы о перечислении денег на лечение и иные благотворительные цели, тщательно не перепроверив всю информацию.

Правила финансовой безопасности в социальных сетях

1. Не привязывайте к соцсетям свою основную платёжную банковскую карту (тем более зарплатную).
2. Не размещайте фото билетов на мероприятия.
3. Не размещайте фото из отпуска с геолокациями.
4. Не демонстрируйте в сети дорогие приобретения и предметы роскоши.
5. Создайте настройки приватности.
6. Включите двухфакторную аутентификацию.
7. Выходите из уч[illegible]спользовали дл[illegible]е устройство.

Финансовое мошенничество

Мошенничество - *хищение* чужого имущества или *приобретение* права на чужое имущество путём *обмана* или *злоупотребление* доверием (*У* *59)*

Мошенничество в сфере компьютерной информации - *хищение* чужого имущества или приобретение права на чужое имущество *путём ввода, удаления, блокирования, модификации* компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей
(*УК РФ, Статья 159.6)*

Куда обращаться при мошенничестве в Интернете

- Написать жалобу в отделение полиции по месту жительства - сотрудники полиции сами направят её по подведомственности.
- Управление «К» МВД России (специализируется на расследовании преступлений в сфере компьютерных технологий). https://mvd.ru/mvd/structure1/Upravlenija/ Upravlenie_K_MVD_Rossii
- Центр безопасности от компании Microsoft. https://www.microsoft.com/ru-ru/security/default.aspx

Спасибо за внимание!