АКЦИОНЕРНОЕ ОБЩЕСТВО
НАЦИОНАЛЬНЫЙ БАНК СБЕРЕЖЕНИЙ

БАЗОВЫЕ ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЛИЧНОЙ ЖИЗНИ

- Два фактора – лучше, чем один. Даже самый надёжный пароль – это всего лишь один фактор. Везде, где это возможно используйте двухфакторную аутентификацию. Обычно она включает логин, пароль и специальный код, приходящий по SMS.
- Хороший пароль – парольная фраза, которая состоит из нескольких слов. Сильные парольные фразы включают в себя заглавные и строчные буквы, цифры, знаки препинания и другие символы.
- Используйте несколько цифровых личностей. Лучше всего, если данные с разных аккаунтов (социальная сеть, онлайн-банк, серверы, удаленный рабочий стол и пр.) будут разными.
- Помните, ваша электронная почта – ключ ко всему. Это ваш паспорт в цифровом мире.
- Всё, что вы выложили в Интернет – останется там навсегда. Эта информация не удаляется. Поэтому подумайте, прежде чем выложить новое фото или другие сведения о себе.
- Удобно или безопасно. Найдите для себя баланс между этими полюсами.
- Если вы пользуетесь сервисом бесплатно – то «товаром» становитесь вы и ваши данные. Это горькая правда, о которой нужно помнить всегда!
- «Это не про меня» – с этой мысли начинаются проблемы. Вы не интересны мошенникам только в том случае, если взломать вас финансово невыгодно.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА РАБОТЕ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Запомните, что преступники в первую очередь атакуют тех, кто имеет прямое отношение к деньгам или может помочь подобраться к таким сотрудникам.
- Business Email Compromise (BEC-атака) – целевая кампания киберпреступников. Цель такой атаки – получить доступ к корпоративной учетной записи электронной почты, чтобы обмануть получателей писем, используя приемы социальной инженерии. На сегодня это самая действенная и самая частая атака в корпоративном сегменте.
- Защиты от приёмов социальной инженерии нет! Нужно постоянно сохранять бдительность.

ПРИ УДАЛЁННОЙ РАБОТЕ И В КОМАНДИРОВКАХ

- Бесплатный интернет – это бесплатный сыр в мышеловке. По возможности не используйте его!
- Если это невозможно, то обязательно используйте VPN. Эта технология была создана, чтобы безопасно работать через небезопасный канал связи.
- Не обменивайтесь важной информацией в открытом виде. Для обмена создавайте хотя бы запароленные архивы.
- Большинство утечек данных происходят из-за того, что вы не знаете, как работает технология/сервис. Узнавайте и не торопитесь устанавливать даже проверенные приложения, плагины и т.п.

ПРИ РАБОТЕ ИЗ ДОМА

- Старайтесь не смешивать работу и личную жизнь. Разделяйте личные и корпоративные: учётные записи, пароли, устройства.
- Если вы вынуждены работать с домашнего компьютера, сперва позаботьтесь о его безопасности. Установите последние обновления для операционной системы и антивируса.
- Помните, что информация передаётся по цепочке. Поэтому работая из дома, считайте, что вы в командировке и применяйте все правила из предыдущего раздела.

АКЦИОНЕРНОЕ ОБЩЕСТВО
НАЦИОНАЛЬНЫЙ БАНК СБЕРЕЖЕНИЙ

БЕРЕГИТЕ СВОЮ УНИКАЛЬНОСТЬ!

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся:

фамилия, имя, отчество;
дата рождения;
место рождения;
место жительства;
номер телефона;
адрес электронной почты;
фотография;
возраст и пр.

КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат действительно тот, за кого себя выдает.
4. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
5. Старайтесь периодически менять пароли.
6. Заведите себе два адреса электронной почты - частный, для переписки (который вы никогда не публикуете в общедоступных источниках), и публичный для открытой деятельности (форумов, чатов и так далее).

КАК ОБЩАТЬСЯ В СЕТИ

1. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, учебы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.
2. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.
3. Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни.
4. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, не используйте нецензурную лексику – читать такие высказывания так же неприятно, как и слышать.
5. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.
6. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.
7. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.
8. Не используйте Сеть для распространения сплетен, угроз или хулиганства.

АКЦИОНЕРНОЕ ОБЩЕСТВО
НАЦИОНАЛЬНЫЙ БАНК СБЕРЕЖЕНИЙ

ПРАВИЛЬНЫЙ ПАРОЛЬ, ЭТО ЗАЩИТА!

Надежный пароль – это главный барьер, который мешает взломать большинство ваших аккаунтов в сети. Если вы не пользуетесь современными методиками создания паролей, то вполне возможно, что мошенники смогут подобрать их буквально за несколько часов. Чтобы не подвергать себя риску кражи данных и не стать жертвой вымогательства, вам нужно создавать пароли, которые могут противостоять усилиям хакеров, вооруженных современными средствами взлома.

КАК СОЗДАТЬ НАДЕЖНЫЙ ПАРОЛЬ:

1. Постарайтесь создать пароль длиной как минимум 10-12 символов, а лучше длиннее.
2. Избегайте простых последовательностей («12345», «qwerty») – такие пароли подбираются за считаные секунды. По той же причине избегайте распространенных слов («password1»).
3. Заглавные и строчные буквы, символы, цифры – всем им найдется достойное место в вашем пароле. Чем больше в пароле разнотипных символов, тем он менее предсказуем.
4. Кодовые фразы надежнее, если слова в них идут в неожиданном порядке. Даже если вы используете обычные слова, берите такие, которые не связаны друг с другом по смыслу, и расставляйте их нелогичным образом. Это поможет противостоять словарному подбору.
5. Составляйте пароль так, чтобы он был понятен вам, но труден для машинного подбора. Даже случайные наборы символов можно запомнить, если они хоть сколько-нибудь читаемы, а также благодаря мышечной памяти. Но вот пароль, который не пустит в ваш аккаунт даже вас самих, бесполезен.
6. Повторное использование паролей может скомпрометировать сразу несколько аккаунтов. Каждый пароль должен быть уникальным.
7. Используйте пароль из буквенных слов, в которых первые две буквы заменяются цифрами и символами. Выглядит это так: «?4 ей#2ка?6цо» вместо «улейрукалицо».

КАК ПОЛЬЗОВАТЬСЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

БЕЗОПАСНОСТЬ:

1. Создавайте разные аккаунты электронной почты под разные задачи.
2. Используйте сложные пароли.
3. Используйте шифрование при получении и отправке.
4. Используйте двухфакторную авторизацию.
5. Не открывайте письма от неизвестных вам отправителей.
6. Не открывайте вложенные файлы без уверенности в их содержании.
7. Используйте программы по защите от вредоносного кода, проверяющие почтовые сообщения.
8. Постоянно обновляйте программы по защите от вредоносного кода.
9. Будьте бдительны.

КАК ЭФФЕКТИВНО ОБРАБАТЫВАТЬ ЭЛЕКТРОННУЮ ПОЧТУ, ЧТОБЫ НИЧЕГО НЕ ПОТЕРЯЛОСЬ:

1. В папке Входящие не должно быть писем! Эта папка для первоначальной сортировки.
2. Из этой папки СПАМ удаляется, а нормальные письма перекладываются в папку «В работе» или «Отработанные».
3. Папка «В работе» не должна содержать более 25 писем, иначе в этом потом заваляется что-нибудь важное.
4. Папок «В работе» может быть много. Можно разбить по темам папки в Работе.
5. Отработанные содержит письма, не требующие ответа или письма, на которые был дан ответ. Опять же, может быть, несколько подобных папок по темам.
6. Отправленные письма сортируются по такому же принципу.

АКЦИОНЕРНОЕ ОБЩЕСТВО
НАЦИОНАЛЬНЫЙ БАНК СБЕРЕЖЕНИЙ

ОСТОРОЖНО! ТЕЛЕФОННЫЕ МОШЕННИКИ!

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно - телекоммуникационных технологий стремительно набирают силу.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости (стяжательство, алчность), чувства (сострадание, обеспокоенность за близких, жалость) в своих корыстных интересах.

ОБЩИЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ТЕЛЕФОННЫХ ПЕРЕГОВОРАХ, КОТОРЫЕ НАДО ПРИМЕНЯТЬ ВСЕГДА:

1. Старайтесь не принимать звонки от неизвестных абонентов;
2. Проверяйте свои контакты в телефоне;
3. Если сомневаетесь прекратите разговор и положите трубку.
4. Никогда и никому не сообщайте:
   - реквизиты ваших документов (паспорт, СНИЛС, ИНН и др.);
   - данные вашей банковской карты;
   - коды, полученные через SMS;
   - адреса места жительства, работы, учебы и др.
5. Не переходите по ссылкам, QR кодам, полученным через SMS, если вы точно в них не уверенны.
6. Не совершайте никаких действий по инструкциям звонящего.
7. Действуйте обдуманно, не торопливо.

КАК РАСПОЗНАТЬ ТЕЛЕФОННЫХ МОШЕННИКОВ

1. Звонящий с неизвестного номера представляется:

- сотрудником Банка;
- сотрудником правоохранительных органов;
- сотрудником социальных служб;
- сотрудником государственных и муниципальных учреждений.

2. Звонящий с неизвестного номера предлагает вам:

- принять участие в расследовании и никому об этом не сообщать;
- сообщить информацию о ваших документах, адресах, реквизитах банковских карт, номерах счетов, кодах из полученных SMS;
- перевести ваши средства на надежный счет;
- разблокировать, заблокировать вашу карту;
- принять информацию о несчастных случаях с вашими родственниками, знакомыми, коллегами по работе.

3. Звонящий с неизвестного номера:

- использует специальную терминологию;
- торопит, создает эффект паники, подталкивает к быстрым действиям;
- выманивает ваши личные данные и сведения;
- ссылается на законы, на нормативные документы;
- угрожают потерей денег.

4. Мошенники используют наши слабости: страх, жадность, невнимательность и некомпетентность.

АКЦИОНЕРНОЕ ОБЩЕСТВО
НАЦИОНАЛЬНЫЙ БАНК СБЕРЕЖЕНИЙ

КТО ТАКИЕ ДРОППЕРЫ

Дроппер или дроп - это человек, который вольно или невольно оказывает услуги мошенникам. Именно на карты дропперов обманутые люди переводят средства на так называемые «безопасные счета». Дальше эти деньги проходят через цепочку переводов и впоследствии обналичиваются. К дропперам относят тех, кто снимает деньги с чужих карт в банкоматах и тех, кто передает свои карты скупщикам. Такую «работу» могут предлагать студентам, нуждающимся гражданам, социально неблагополучным людям и даже школьникам, у которых банковские карты могут появляться с 14 лет с согласия родителей. Привлекают их легкими заработками при минимуме усилий. При этом человек может даже не подозревать, что его вовлекли в преступную схему.

ЧТО ДЕЛАЮТ ДРОППЕРЫ

На дропперов оформляются банковские карты (дроп-карты), через которые телефонные мошенники переводят, затем обналичивают украденные с других банковских карт средства. Далее деньги зачисляются на другой «пластик» или же через спецсервисы конвертируются в криптовалюту. Это могут делать как сами дропперы, так и их «хозяева».
Так же дроперы предоставляют доступ мошенникам к своему личному кабинету в Банке, мобильному приложению. За участие в финансовой афере дроп получает процент от обналиченной суммы.

Чаще всего быть дропперамии соглашаются:

- студенты;
- мигранты из деревень, маленьких городов;
- иммигранты из экономически неразвитых стран;
- другие уязвимые слои населения (сироты, многодетные семьи, безработные).

КАК ПОНЯТЬ, ЧТО ЧЕЛОВЕКУ ПРЕДЛАГАЮТ СТАТЬ ДРОППЕРОМ?

Предложения могут быть самые разные: под видом банков, которым нужно выполнить «план по продажам», предлагают людям оформить любую карту и передать ее неким лицам за вознаграждение — например, за 3 тыс. рублей. Затем включается сетевой маркетинг: приведи друга с картой и получи еще 2 тыс. рублей. Таким способом дети массово втягиваются в дропперство. В некоторых случаях подросток физически не передает мошеннику «пластик», а предоставляет ему реквизиты карты и коды доступа к онлайн-банкингу.

Еще один из вариантов привлечения - школьникам или студентам предлагают «трудоустройство»: быть администратором лотереи и якобы отправлять выигрыш победителям. На самом деле карта человека используется в схеме вывода похищенных денег, и он оказывается соучастником преступления. Стоит насторожиться, если предлагают работу вне зависимости от образования и опыта, если обещают быструю и легкую прибыль, связанную с получением денег на ваш счет и последующим переводом по реквизитам.

ПОСЛЕДСТВИЯ ДЛЯ ДРОППЕРОВ

- Привлечение к уголовной и административной ответственности.
- Попадание в базы антифрод-систем, что значительно сократит ваши возможности по использованию банковских продуктов.
- Вовлечение в криминальные структуры.