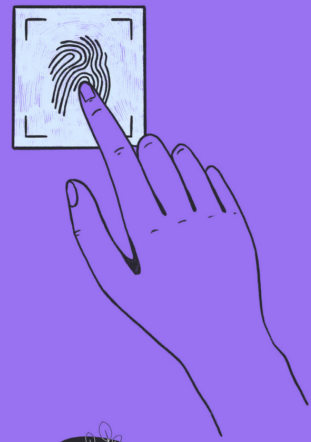
Электронный учебник

Кибер безопасность

Как защитить личные и корпоративные цифровые активы



Живое Обучение

Александр Николаевич Панкрушин

Кибербезопасность. Как защитить личные и корпоративные цифровые активы

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=68840739
Кибербезопасность.Как защитить личные и корпоративные цифровые активы / Панкрушин Александр Николаевич: ЛАБОРАТОРИЯ ЗНАНИЙ; Москва; 2022

Аннотация

Электронный учебник – сборник материалов, изучив который вы сможете получить краткое и емкое представление о личной и корпоративной кибербезопасности.

– Какие тактики применяют кибермошенники?

– Как грамотно противостоять манипуляциям кибермошенников?

– Как распознавать фишинговые письма и не переходить по вредоносным ссылкам, защищать свои данные и безопасно общаться в соцсетях?

На изучение вам потребуется 50 минут. В конце вас ждут вопросы для проверки усвоения материала

В формате PDF A4 сохранен издательский макет книги.

Содержание

Александр Панкрушин
Кибербезопасность. Как защитить личные и корпоративные цифровые активы

Про электронный учебник

Что вас ждет?
Фокус внимания
Советы по обучению
∞

Что вас ждет?

Электронный учебник – сборник материалов, изучив который вы сможете получить краткое и емкое представление о личной и корпоративной кибербезопасности.

Контент электронного учебника сформирован на базе разнообразных источников. В нем, помимо правил кибербезопасности, вы найдете:

– вопросы на проверку понимания изученного;

– краткие резюме и памятки;

– советы по применению;

– рекомендации по дополнительному чтению;

– реальные примеры атак кибермошенников на известные компании;

– многочисленные правила, продемонстрированные на практических кейсах.

На изучение вам потребуется 50 минут. В конце вас ждут вопросы для проверки усвоения материала

∞

Фокус внимания

Этот электронный учебник разработан именно для вас. Чтобы эффективно фокусироваться и хорошо запоминать материал, перед началом обучения и в начале каждой темы спросите себя:

Что я хочу сейчас изучить? Какие у меня есть вопросы?

Цель электронного учебника – не в изучении как таковом. Полученные знания важно применять на практике, в работе и в личной жизни. Верный способ это сделать – начать пользоваться изученным уже сегодня.

В конце учебника или отдельной темы попробуйте ответить на несколько вопросов:

– Какие знания и навыки я получил в пройденной теме/в учебнике?

– Как я могу использовать изученное в работе и в жизни?

– Когда я могу начать применять новые знания и с чего я начну?

✎ Старайтесь записывать свои мысли в начале и в конце каждой темы. По завершении чтения всего учебника просмотрите записи и начните действовать. У вас обязательно получится!

∞

Советы по обучению

Эти приемы помогут значительно усилить эффект от обучения.

– Изучайте материал последовательно, чтобы ничего не упустить.

– Уделите обучению достаточно времени. Если сейчас у вас нет свободных 50 минут, запланируйте обучение на то время, когда они у вас будут.

– Делайте перерывы каждые 15–20 минут – так вы гораздо лучше усвоите материал.

– Постарайтесь не отвлекаться, сосредоточьтесь на изучении материала.

– Во время чтения делайте записи, зарисовки, схемы.

– Чтобы лучше ориентироваться в учебнике и запоминать материал, перед началом обучения уделите внимание “Содержанию” и изучите структуру.

– Найдите дополнительную информацию по теме и попробуйте обсудить ее с коллегами или друзьями.

Как только вы изучите весь материал, постарайтесь поставить себе такую задачу, которая поможет опробовать новые навыки на практике.

Подробнее о теме

Почему тема важна, и что лежит в основе учебника?
Что вы изучите?
∞

Почему тема важна, и что лежит в основе учебника?

«Последствия того, что можно назвать кибервойной, – целевых атак на больницы, аэропорты, финансовые системы и промышленные предприятия – могут быть чудовищными.»

Евгений Касперский, генеральный директор «Лаборатории Касперского». Фото: Kaspersky. Kaspersky, CC BY-SA 4.0 https://bit.ly/3prDySB

Мы живем в современном цифровом мире, где зависим от информационных технологий больше, чем когда-либо, и наше здоровье, счастье и даже наша жизнь связаны с ними. Независимо от того, используем ли мы медицинское оборудование в больницах, путешествуем на новейших автомобилях, пользуемся системами безопасности в наших домах или супертехнологичными смартфонами – компьютеризированное оборудование с каждым годом играет все большую роль в современном человеческом опыте.

Можно сказать, что информационная безопасность сегодня становится основной потребностью человеческой жизни.

Если вы тратите на кофе больше, чем на информационную безопасность, то вас взломают. Более того, вы заслуживаете того, чтобы вас взломали.»

Ричард Кларк, бывший советник администрации президента США, специалист по борьбе с терроризмом. Фото: Richard A. Clarke, https://richardaclarke.net

Несмотря на актуальность темы, многие до сих пор склонны недооценивать угрозы кибератак, относиться беспечно к своему поведению. А множество мифов и заблуждений, окружающих кибермошенников, приводят к контрпродуктивным суждениям и поведению.

О том, как быть более защищенным от уловок кибермошенников, какие действия нужно предпринимать, каких заблуждений избегать, пишут многие издания. Среди них:

– Блог Kaspersky Daily. Источник статей, обзоров и рекомендаций в области информационной безопасности от «Лаборатории Касперского» – международной компании, специализирующейся на разработке систем защиты от компьютерных вирусов, спама, хакеров и прочих киберугроз. Входит в четверку ведущих мировых производителей программного обеспечения для защиты конечных устройств.

– Портал РБК Pro. Раздел «Кибербезопасность». Авторитетный источник с лекциями и интервью признанных экспертов, переводами статей западных изданий, кейсами, ис-

следованиями и прогнозами.

Именно эти источники положены в основу учебника.

∞

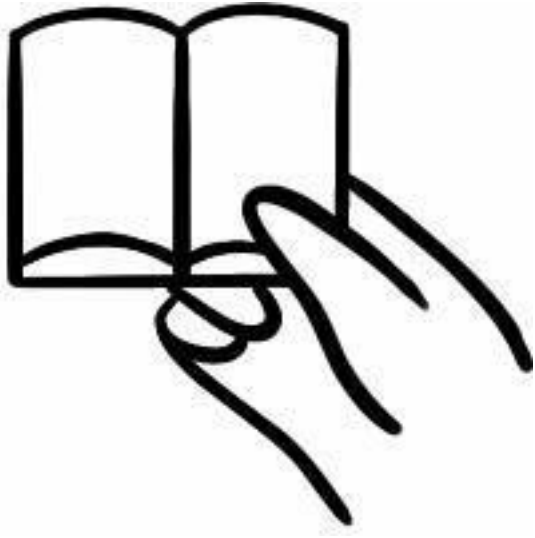
Что вы изучите?

Вам предстоит узнать:

1. Какие тактики используют кибермошенники и как с ними бороться;
2. Как предотвратить утечку конфиденциальных данных на ноутбуках, смартфонах и других устройствах;
3. Как распознавать фишинговые письма, поддельные сайты, опасные ссылки;
4. Как использовать, хранить и передавать конфиденциальную информацию;
5. Как создавать надежные пароли и правильно с ними обращаться;
6. Как безопасно общаться в соцсетях и серфить в интернете.

Желаем эффективного и полезного обучения!

Глава 1
Можем ли мы стать защищеннее?



Вы изучите:

– Какие методы используют кибермошенники и как им противостоять?

После изучения вы сможете:

– понять, с помощью каких трюков кибермошенники втираются к нам в доверие;

– осознать ответственность за игнорирование правил безопасности;

– использовать «золотое правило» противодействия манипуляциям.

∞

Какие методы используют кибермошенники и как им противостоять?

Вначале рекомендуем сфокусировать свое внимание и ответить на следующий вопрос:

Что я хочу сейчас изучить? Какие у меня есть вопросы?

Остановитесь и задумайтесь

Подумайте над ситуацией: представьте, что в разгар рабочего дня вы заходите в свою электронную почту и видите следующее письмо:

Как вы поступите?

Дадим вам небольшую подсказку
Среди вариантов ниже есть один приемлемый:
– можно скачать файл;
– можно перейти по ссылке;
– можно ничего не делать и удалить письмо.

Попробуйте самостоятельно ответить на вопрос, прежде чем перевернуть страницу и посмотреть рекомендуемый ответ.

Решение ситуации

Здорово, если в своих размышлениях вы склонялись к варианту **«ничего не делать и удалить письмо».**

Почему?

Дело в том, что адрес, с которого пришло письмо – sberbankru.ru – не настоящий сайт Сбербанка. Нажав на ссылку или скачав и открыв файл на своем устройстве, вы рискуете запустить вредоносный код, который может использовать уязвимости в вашей операционной системе и повредить файлы, а за восстановление кибермошенник попросит деньги.

Если вы не пошли на поводу у кибермошенника, вам может показаться, что ничего страшного и не случилось. Однако получение подобных писем, особенно в большом количестве, может свидетельствовать о готовящейся массированной кибератаке как на вас, так и на вашу компанию. При этом предотвратить мошеннические действия не настолько сложно, но для этого важно знать врага в лицо.

Атаки, как на частных лиц, так и на крупные компании, происходят, как правило, при невольном содействии/бездействии обычных людей – сотрудников.

Несколько громких случаев, доказывающих это.

Примеры из реальной жизни

Пример 1. Взлом компании Sony Pictures Entertainment. 2014 год

Хакерская группа Guardians of Peace изучила профили сотрудников компании в LinkedIn и разослала им письма с файлами, в которых содержался вирус. Сотрудники скачали файлы, и, попав на корпоративные компьютеры киностудии, вирус позволил злоумышленникам месяцами вести слежку и удаленно управлять устройствами.

Вскоре хакеры опубликовали в Сети несколько еще не выпущенных фильмов студии: «Ярость», «Энни», «Уильям Тернер», «Все еще Элис» и другие. Кроме того, злоумышленники похитили личные данные 3803 сотрудников Sony Pictures Entertainment и членов их семей, содержимое внутренней электронной почты, информацию о заработной плате и копии неизданных фильмов.

Пример 2. Атака на сеть отелей Marriott International. 2014–2018 годы

В 2014 году хакеры взломали систему Starwood Preferred Guest, где хранились данные о клиентах отелей Marriott: имена и фамилии, номера паспортов, контактные и платежные данные. Доступ к базе данных осуществлялся через учетные записи, созданные в системе. Атака вскрылась лишь четыре года спустя.

Пострадали около 500 млн клиентов. Сети пришлось заплатить $124 млн штрафа за утечку данных.

Пример 3. Утечка данных пользователей Yahoo

в 2013–2014 годах

В результате хакерской атаки на Yahoo в 2013 году были похищены личные данные около 1 млрд пользователей. Злоумышленники могли получить доступ к именам, электронным адресам, телефонным номерам, датам рождения, а также проверочным вопросам и ответам, которые необходимы для восстановления забытого пароля.

В 2016 году компания Yahoo сообщила, что похожий эпизод был зафиксирован в конце 2014 года. Тогда хакеры взломали не менее 500 млн аккаунтов.

Позже Yahoo пересмотрел оценку количества пострадавших, включив в нее все 3 млрд учетных записей пользователей. По оценкам экспертов, эти нарушения снизили стоимость компании на 350 миллионов долларов.

Пример 4. Взлом автомобилей Tesla. 2016 год

В 2016 году китайская хакерская группа взломала Tesla Model S через точки доступа Wi-Fi: они предлагали водителям подключиться к Wi-Fi, а потом устанавливали вредоносное ПО и получали полный контроль над системами управления, в том числе над системой тормозов. Tesla устранила неисправность, но в последующем обнаруживались новые уязвимости.

В августе 2020 года хакер Егор Крючков попытался внедрить вредоносное ПО в систему управления Tesla. Он предложил сотруднику компании взятку $1 млн, но хакера осудили на 5 лет.

Кто виноват во взломах?

Как вы могли заметить, и случаи атак на обычных людей, и громкие кибератаки объединяет одно – в основном мы сами совершаем действия, которые позволяют кибермошенникам получать доступ к нашим ценностям.

Без вашей помощи кибермошеннику не проникнуть на ваше устройство и не завладеть вашими и корпоративными ценностями!

В этом смысле мошенники похожи на вампиров. Как гласят легенды, вампиры не могут войти в дом человека, пока он сам их не впустит. Так же и с киберпреступниками.

Конец ознакомительного фрагмента.