30 ноября – Международный день защиты информации

В ноябре 1988 года прошла первая массовая компьютерная эпидемия – так называемая эпидемия червя Морриса*. В этом же году 30 ноября был объявлен международным Днем защиты информации (Computer Security Day). Таким образом, Американская ассоциация компьютерного оборудования решила напомнить всем о том, *что необходимо защищать компьютерную информацию и обратила внимание производителей и пользователей на проблему безопасности*. С тех пор 30 ноября проводятся международные конференции по защите информации, сопровождаемые массой интересных мероприятий.

*Червь Морриса – сетевой червь, парализовавший работу шести тысяч интернет-узлов в США. Этот червь был наречён червём Морриса по имени его автора – аспиранта факультета Вычислительной техники Корнелльского университета Роберта Т. Морриса.

Ущерб от червя Морриса был оценён примерно в 96,5 миллионов долларов. Сам Моррис хорошо законспирировал код программы, и вряд ли кто мог доказать его причастность. Однако его отец, компьютерный эксперт Агентства национальной безопасности, посчитал, что сыну лучше во всём сознаться. На суде Роберту Моррису грозило до пяти лет лишения свободы и штраф в размере 250 тысяч долларов, однако, принимая во внимание смягчающие обстоятельства, суд приговорил его к трём годам условно, 10 тысячам долларов штрафа и 400 часам общественных работ.

С тех пор минули десятилетия. Всё компьютеризовано, в мире миллиарды сотовых телефонов, новейшей техники, фотоаппараты, телевизоры, космическая станция. И их защита всё нужнее и нужнее. Ведь враг силен: в дни хакерских атак крушатся серверы телекомпаний, банков, правительств, идет грабеж с пластиковых карт, банковских счетов. Выдумываются и выдумываются новые версии обмана человечества.

И всему этому надо противостоять.

Если говорить о праздниках вообще, то они имеют отношение к определенной категории людей. ДЕНЬ ЗАЩИТЫ ИНФОРМАЦИИ – не из тех. Это – общий праздник, в котором заинтересованы мы все! Так давайте в меру сил и возможностей поддерживать его!

Как не стать жертвой киберпреступника:

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ 01

НЕОБХОДИМО:

+ Создавать персональные (уникальные) пароли к разным сервисам
+ Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
+ Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

× Использовать повторения символов
× Хранить пароли на бумажных носителях
× Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
× Сохранять пароль автоматически в браузере
× Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

+ Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет
+ Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
+ Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

× Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ 03

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

6 правил информационной безопасности

GROUP-IB

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 04

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
+ Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

× Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники

× Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

+ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
+ Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

× Размещать персональную и контактную информацию о себе в открытом доступе

× Использовать указание геолокации на фото в постах

× Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса

× Употреблять ненормативную лексику при общении

× Устанавливать приложения с низким рейтингом и отрицательными отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ 06

+ Хранить в тайне пин-код карты
+ Прикрывать ладонью клавиатуру при вводе пин-кода
+ Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
+ Использовать услугу «3-D Secure» и лимиты на максимальные суммы онлайн-операций
+ Скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

× Хранить пин-код вместе с карточкой / на карточке

× Сообщать CVV-код или отправлять его фото

× Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»

× Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.