ГЛОССАРИЙ

АНТИВИРУСНОЕ ПО — программа, которая находит на устройстве и в трафике зараженные файлы и лечит их: удаляет вирусы и исправляет поврежденную информацию.

АНТИВИРУСНАЯ БАЗА — база, содержащая информацию о вирусах, необходимую, чтобы найти их и обезвредить.

АРХИВ — файл, содержащий в себе один или несколько других файлов в специальной сжатой форме.

АУТЕНТИФИКАЦИЯ — процедура проверки подлинности.

БАЗА ДАННЫХ — информационная модель, хранящая данные о группе объектов.

БАНК-КЛИЕНТ — система электронных расчетов, позволяющая пользователям удаленно управлять своими финансами.

БЕСПРОВОДНАЯ СЕТЬ — технология, позволяющая создавать сети, полностью соответствующие стандартам обычных проводных сетей, но без использования кабельной проводки.

ВИРУС — вредоносная программа, которая создает копии самой себя и заражает другие программы, добавляя в них свой код.

ВНЕШНИЕ ИСТОЧНИКИ ИНФОРМАЦИИ — интернет, социальные сети, электронная почта.

ИНТЕРНЕТ — глобальная компьютерная сеть, которая связывает между собой пользователей компьютеров во всем мире.

ГЛОССАРИЙ

МОБИЛЬНОЕ УСТРОЙСТВО — смартфон или планшет.

НОСИТЕЛЬ — объект, используемый для хранения и передачи информации.

ОНЛАЙН-ПЛАТЕЖ — оплата товаров и услуг в интернете или с помощью мобильных приложений.

ПК — персональный компьютер.

ПОРТ ПК — порт для подключения внешних устройств к ПК.

ПРОГРАММА — последовательность инструкций, определяющих процедуру решения конкретной задачи компьютером

РЕЗЕРВНОЕ КОПИРОВАНИЕ — процесс создания копии данных с целью их восстановления в случае повреждения или удаления.

СОЦИАЛЬНАЯ СЕТЬ — интерактивный веб-сайт, содержание которого создается самими участниками сети.

СРЕДСТВО АУТЕНТИФИКАЦИИ (E-ТОКЕН) — устройство для проверки принадлежности субъекту доступа предъявленного им идентификатора.

СТАЦИОНАРНОЕ УСТРОЙСТВО — ПК, не предназначенный для перемещения.

ФИНАНСОВЫЕ ТРАНЗАКЦИИ — операции с денежными средствами на банковском счете.

KASPERSKY lab

Как не навредить компании по незнанию?

Рекомендации специалистов «Лаборатории Касперского» по обеспечению безопасности рабочего места

ИСПОЛЬЗУЙТЕ ЛИЦЕНЗИОННОЕ АНТИВИРУСНОЕ ПО и вовремя обновляйте антивирусные базы на всех устройствах

Регулярно **ОСУЩЕСТВЛЯЙТЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ** данных на всех устройствах

Регулярно **УСТАНАВЛИВАЙТЕ ОБНОВЛЕНИЯ СТОРОННЕГО ПО** на всех устройствах

Регулярно **МЕНЯЙТЕ ПАРОЛИ** на всех устройствах; пароли должны содержать не менее 8-12 символов, строчные и прописные буквы, цифры и другие знаки

ПРОВЕРЯЙТЕ ВСЕ ФАЙЛЫ из входящей электронной почты и социальных сетей на вирусы перед тем, как открыть их

НЕ ОТКРЫВАЙТЕ ПОДОЗРИТЕЛЬНЫЕ ВЛОЖЕНИЯ в электронной почте и социальных сетях, особенно если это архивы или исполняемые файлы (.exe)

Обязательно **ПРОВЕРЯЙТЕ НА ВИРУСЫ ЛЮБОЙ НОСИТЕЛЬ** при подключении к ПК

МИНИМИЗИРУЙТЕ РАБОТУ С ВНЕШНИМИ ИСТОЧНИКАМИ ИНФОРМАЦИИ на компьютере, где установлен банк-клиент

ВЫНИМАЙТЕ СРЕДСТВА АУТЕНТИФИКАЦИИ из портов ПК по завершении работы с банк-клиентом

НЕ ПРОВОДИТЕ ФИНАНСОВЫЕ ТРАНЗАКЦИИ в публичных местах с бесплатным беспроводным интернет-доступом (Wi-Fi)

По возможности **ИСПОЛЬЗУЙТЕ SMS-АУТЕНТИФИКАЦИЮ** при совершении любых онлайн-платежей

Никогда **НЕ ПЛАТИТЕ ЗЛОУМЫШЛЕННИКАМ ВЫКУП** в случае блокировки компьютера или данных