Автор:
14.11.2007 23:05

Фишинг - вид мошенничества с целью хищения личных сведений. Пользователь получает электронное письмо из якобы надежного источника с просьбой раскрыть такие сведения, как данные о банковском счете и номера и пароли кредитных карт. Фишеры подделывают доменные имена банков и других компаний, с тем, чтобы обмануть клиентов, которые думают, что посетили надежный Web-сайт.

Мошенники создают адреса Web-узлов, которые выглядят, как адреса Web-узлов, вызывающих доверие, однако на самом деле такие адреса незначительно видоизменены. Такие адреса называют омографами Доменное имя составляется при помощи букв алфавитов разных языков, а не только при помощи английского алфавита. К примеру, Web-адрес «www. niicrosoft. com» , на первый взгляд, выглядит нормально, но в действительности английская буква «I» была заменена другой буквой "i» - символом кириллицы. Выявить такой подлог крайне сложно.

Не поддавайтесь на провокации мошенников, приглашающих вас посетить Web-сайт, который выглядит, точь-в-точь как официальный сайт. Никогда не отвечайте на присланные по электронной почте просьбы сообщить ваши личные сведения. Большинство компаний никогда не станут запрашивать личную информацию по электронной почте. Если вы получили подозрительное электронное сообщение, обратитесь в соответствующую службу, чтобы проверить таков сообщение.

Спам представляет собой сообщения, массово рассылаемые людям, не выразившим желание их получать. Спаммеры собирают адреса электронной почты с различных Web-сайтов и из других источников. Чтобы избежать атак спаммеров, используйте несколько различных адресов электронной почты. Например, один адрес для заполнения Web-форм и другой адрес для личной переписки. Также старайтесь не подписываться на массовые рассылки. Дополнительную информацию о борьбе со спамом вы можете получить в Справке Microsoft Office и Microsoft Windows.

Шпионящее ПО - программное обеспечение, предназначенное для сбора личных сведений без ведома и разрешения пользователя. Как правило, программы-шпионы загружаются и устанавливаются на компьютер вместе с бесплатным программным обеспечением - таким, как свободно распространяемое программное обеспечение, игры или различные музыкальные программы. Шпионящее программное обеспечение часто

ассоциируют с бесплатными программными продуктами с размещенной в них рекламой, то есть с продуктами, которые отображают рекламные объявления (например, всплывающие рекламные окна). Примером шпионящего программного обеспечения и вредоносных рекламных программ могут служить программы, которые изменяют домашнюю страницу пользователя или страницу поиска без разрешения пользователя. Чтобы избежать проблем, связанных с установкой шпионящего программного обеспечения и бесплатных программных продуктов с размещенной в них рекламой, внимательно читайте разделы лицензионных соглашений на установку программного обеспечения, написанные мелким шрифтом. Также почаще сканируйте свой компьютер на наличие шпионящего и нежелательного программного обеспечения при помощи соответствующих программ обнаружения и удаления такого программного обеспечения (например, Ad-aware от Lavasoft) и обязательно включите функцию блокировки окон. Дополнительную информацию об этом вы можете получить в Справке Microsoft Office и Microsoft Windows.