УГРОЗЫ В ИНТЕРНЕТЕ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Қулмаматов Синдорқул Ибрагимович ГулГУ, заведуший кафедры
Абдураимов Достонбек Эгамназар ўғли ГулГУ, преподаватель
Норматова Малика Норқуловна ГулГУ, преподаватель
Монасипова Рената Фидановна ГулГУ, преподаватель

Аннотация: Суть этой статьи состоит в том, чтобы обсудить положительные и отрицательные последствия использования Интернета в современном информационном обществе, а также то, почему он необходим и каковы его преимущества. Однако удобство и преимущества, которые Интернет предоставляет людям, не являются только они, но также и тип сети, который создает множество проблемных ситуаций.В статье подробно рассказывается о том, как преодолеть эти удобства и проблемные ситуации.

Ключевые слова:Интернет, телефон, компания, электронная почта, кибер, банк, кредитная карта.

Abstract: The essence of this article is to talk about the positive and negative consequences of using the Internet in today's information society, as well as why the Internet is needed and what its benefits are. However, the convenience and benefits that the Internet provides to people are not only these, but also the type of network that creates a variety of problematic situations. The article provides details on how to overcome these conveniences and problematic situations.

Key words: Internet, telephone, company, email, cyber, bank, credit card.

Самая большая угроза для пользователей Интернета - это риск того, что их личная информация попадёт в руки других пользователей или будет раскрыта. Мы вводим большую часть нашей личной информации в Интернет, когда пользуемся онлайн-сервисами, общаемся в социальных сетях или по электронной почте. Это могут быть личные фотографии, банковская или финансовая информация, информация о здоровье, наша конфиденциальная

переписка с друзьями или электронные письма, логины и пароли, используемые для доступа к определенным сайтам.

Как правило, безопасное хранение этой информации обеспечивается сайтами, предоставляющими онлайн-услуги, но также бывают случаи, когда ваша информация может попасть в руки нежелательной третьей стороны, и они могут использовать эту информацию в злонамеренных целях.

Это означает, что вся информация, которая принадлежит только нам и не передается другим лицам без нашего согласия, является нашей личной собственностью, и мы имеем право на личную неприкосновенность в отношении нее. Раскрытие личной информации может происходить не по вашей вине или в результате действий конкретного злоумышленника или отдельных лиц, например хакеров. Раскрытие личной информации может нанести вам материальный и моральный ущерб.

Например, вы разместили личную фотографию или информацию в общественном месте, полагая, что вы отправляете их только другу, не понимая процедуры использования социальной сети.

Или вы нажимали на сомнительные ссылки, размещенные на определенных сайтах в социальных сетях, думая, что они никому не будут видны; вы неосознанно поделились им на своей странице или по неосторожности открыли подозрительный сайт, чтобы информация об этом сайте появилась на вашей общедоступной странице без вашего согласия. Раскрытие такой информации о вашей личной жизни другим лицам может нанести ущерб вашей репутации или вызвать у других негативное впечатление о вас. Это моральный ущерб. Также из-за такой невнимательности они могут посещать различные запрещенные сайты от вашего имени.

Если вы щелкнете ссылку в подозрительном электронном письме и откроете его, и в результате на вашем компьютере будет установлено вредоносное программное обеспечение, целью которого является кража личной информации, оно может скопировать всю личную информацию на ваш компьютер и электронную почту и отправить ее по адресу люди,

стоящие за этой программой. Похищенные данные могут включать информацию о банках и кредитных картах, и используя их, киберпреступники могут украсть ваши деньги.

На вопрос, что такое кибератака и кто за ней стоит, можно ответить следующим образом. За интернет-атаками, нацеленными на обычных людей, в основном стоят преступники или группы, стремящиеся разбогатеть. Они взламывают электронные письма людей, компьютеры или другие электронные устройства и крадут личную информацию, тем самым находя информацию об их банке или кредитной карте и крадя у них деньги.
Они также могут вымогать деньги, шантажируя людей угрозой кражи личной информации, фото и видео и их распространения.

В то же время государственные учреждения также широко используют Интернет для поиска лиц, причастных к незаконной деятельности. Если вы пользуетесь сомнительным или спорным сайтом и онлайн-ресурсами и не знаете, как безопасно ими пользоваться, даже если вы не совершали никакого преступления, вы можете попасть в поле зрения органов безопасности, и это может причинить вам нежелательные неудобства.

Ответ на вопрос, зачем нужна интернет-безопасность, следующий. Важно знать правила безопасного использования Интернета, чтобы избежать неприятных ситуаций, упомянутых выше.

Для предотвращения атак вирусов и вредоносных программ обычно используются специальные программы защиты. Но лучший способ защититься от таких угроз - это соблюдать интернет-гигиену. То есть, если вы знаете правила правильного использования Интернета и можете отличать подозрительные источники от надежных сайтов и знаете, что делать, когда вы сталкиваетесь с ними, у вас меньше шансов стать жертвой кибератак.

Угрозы исходящих через электронную почту, можно разделить на несколько типов: Спам- Любое письмо, приходящее на вашу электронную почту, которое вы не хотите получать, можно назвать «спамом». Как правило, группы, которые собирают адреса электронной почты людей

различными способами, рассылают массовые электронные письма огромному количеству электронных писем. Электронные письма, которые приходят в виде спама, могут быть безвредными, а информация в них может быть только простой рекламой определенного продукта. Однако такие электронные письма считаются «спамом», потому что вы не хотите получать рекламу продуктов компании, и без вашего согласия они получат ваш адрес электронной почты откуда-то и отправят вам эту информацию. Например, вы получаете письмо от фармацевтической компании со списком лекарств и ценами на них. Вы не имеете отношения к этой компании или не являетесь ее клиентом. Это означает, что ваша «электронная почта» где-то зафиксирована и вам отправили письмо с рекламой своей продукции. На самом деле это сообщение не содержит никакой безобидной информации, но как нежелательная информация такое письмо также считается «спамом».

Способы защиты от спама:

Никогда не размещайте свой личный адрес электронной почты в публичных местах - социальных сетях, сайтах и публичных форумах. При использовании Интернет-услуг подписывайтесь только на те сайты, которые, как вы уверены, безопасны и необходимы для вас. То есть не вводите свой адрес электронной почты нигде в Интернете, где вас просят ввести адрес электронной почты, потому что существует множество поддельных сайтов и служб, которые собирают электронные письма для рассылки спама. Не открывайте ссылки на интернет-адреса в спам-письмах. Их можно использовать для установки на ваш компьютер программ, интенсивно использующих данные. Даже не нажимайте на ссылку «Отписаться». Они напишут такие слова, чтобы обмануть вас, то есть на самом деле вы можете переходить по ссылке на адрес, где находится вредоносная программа.

Phishing- этот тип угроз - одна из самых серьезных угроз, которые передаются через электронную почту и нацелены на кражу личной информации людей. “Phishing” эти письма которые создают впечатление, что они были отправлены от имени знакомой вам организации или учреждения.

Например, если вы работаете с банком или финансовым учреждением, они могут написать вам письмо от имени этого банка с запросом вашей личной банковской информации или посетить их веб-сайт по ссылке, чтобы предоставить или получить дополнительную информацию. Если вы перейдете по ссылке в письме, нет никаких сомнений в том, что вредоносное программное обеспечение будет установлено на ваш компьютер. Тот факт, что такие письма написаны профессионально, с изображениями логотипов и физических адресов реальных организаций, не должен вводить вас в заблуждение.

Способы защиты от “Phishing”:

“Phishing” никогда не нажимайте на ссылки которые отображаются в подозрительных электронных письмах. Не отвечайте на такие письма и не отправляйте запрашиваемую информацию (например, информацию о банке и кредитной карте, пароль и т. д.) проверьте структуру письма: написано без профессиональных и орфографических ошибок? Соответствует ли содержание, и форма стилю вашей организации или компании? Помните, что написание без орфографических ошибок не может быть основанием для того, чтобы письмо было верным и убедительным. Если вы не уверены в подлинности письма, прежде чем отвечать на него или открывать в нем ссылку, свяжитесь с организацией или компанией, доставившей письмо, по телефону или другим способом, чтобы проверить, действительно ли письмо пришло от них. Убедитесь, что почтовый адрес, на который отправлено письмо, совпадает с именем и доменом сайта компании, который вам известен. Например, фактическая электронная почта на www.saharschool.org приходит с таких адресов, как info@saharschool.org или admin@saharschool.org. Первая часть может быть любым словом, но обратите внимание на часть, которая идет после значка электронной почты (@).“Phishing” в письмах они могут использовать адрес электронной почты, основанный на других поддельных сайтах, близких к исходному, например saharschol.org или saharschool.com, но не совсем то же самое. То же самое

можно сказать и при проверке подлинности сайтов. Если ссылка в письме скрыта под словом, и вы хотите знать, куда она приведет, наведите указатель мыши на слово, скрытое в ссылке, не нажимая на ссылку. После этого появится ссылка в левом нижнем углу браузера. В зависимости от адреса сайта вы можете сказать, настоящий он или нет. Помните, не открывайте сайт, пока не убедитесь, что он подлинный.

Spoofing – Письма от кого-то, кого вы знаете, но не отправляете, называются Spoofing. Хакеры или вредоносные программы могут контролировать адрес электронной почты знакомого и отправлять вам вредоносные электронные письма от его имени. Или, наоборот, ваш адрес электронной почты может быть скомпрометирован вредоносным ПО, и такие электронные письма могут быть отправлены другим лицам от вашего имени. Это может происходить не только по электронной почте, но также с помощью служб электронной почты или печати сообщений в социальных сетях.

Способы защиты от: “Spoofing”

Если письмо друга или знакомого выглядит подозрительно, не отвечайте на него и не открывайте в нем адрес сайта. Попросите друга связаться с вами по телефону или другим способом связи, чтобы проверить подлинность этого письма. Если вы не знаете, что отправили другим людям “Spoofing” если вы заметили, что письмо было отправлено или отправляется, немедленно измените пароль своей электронной почты и повторно подключитесь к людям, которые оставили сообщение, чтобы предупредить вас, что вы не отправляли письмо. В заключение можно сказать, что преимущества и возможности Интернета для человечества увеличиваются день ото дня. Однако опасения по поводу безопасности не уменьшились. Даже если у вас есть все необходимое программное обеспечение для защиты информации, ваши действия в Интернете никогда не будут безопасными. Вы можете свести к минимуму уровень риска для себя, выбрав надежный пароль или отказавшись от доступа к вредоносным сайтам, но если хакеры намерены

атаковать вас лично, они с меньшей вероятностью переживут угрозу. Конечно, обычным людям практически невозможно подвергнуться преднамеренной атаке хакера. Следовательно, в заключение предлагаем вам следующие рекомендации, чтобы не становиться с угрозами из интернета.

- Как можно реже вводите свою личную информацию на веб-сайтах и в сетях;
- Вводите меньше личной информации на социальных сайтах;
- Используйте компьютер и различные устройства, которые вводят вашу личную информацию как можно тщательнее;
- Не общайтесь с незнакомыми людьми и никогда не открывайте адреса сайтов и прикрепленные файлы в письмах от них;
- Не думайте, что ваши личные письма и разговоры в чате неизвестны никому, кроме вас и человека, с которым вы общаетесь;
- Не занимайтесь противоправной деятельностью в Интернете. Итак, будьте в Интернете законопослушным гражданином.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1.Ш.М.Мирзиёев. Вместе мы построим свободное и процветающее демократическое государство Узбекистан. – Тошкент : Ўзбекистон, 2016. - 56 б.

2.Президент Республики Узбекистан Мирзиёев Ш.М. Постановление № ПФ-4947 от. «Стратегия действий» по пяти приоритетным направлениям дальнейшего развития Республики Узбекистан. Т .: 2017.

3.Левин, Джон, Р., Бароди, Кэрол, Левин-Янг, Маргарет. Internet для “Чайников”, 8-е издание.: Пер.сангл.—М.:Издательскийдом "Вильяме", 2003.—288 с.

4.Абдуганиев А. А. Интернет-технологии. Тексты лекций, Ташкент, 2011, 88 с.