Бюджетное профессиональное образовательное учреждение
Омской области
«Седельниковский агропромышленный техникум»

Исследовательский проект по теме:

«Как защитить себя от фишинга»

Автор:
обучающийся 41 группы
по специальности 35.02.07.
«Механизация сельского хозяйства»
Зуевский Дмитрий

Руководитель:
Щербицкая О.В.

Седельниково – 2020

ОГЛАВЛЕНИЕ.

Введение

Мы живем в мире, который постоянно меняется, совсем за недолгий промежуток времени человек изобрел много нового. Сравнительно недавно, Интернет был не так сильно распространён, как сейчас, люди даже мечтать не могли о быстрой и безлимитной работе в Сети. Сейчас она очень прочно вписалась в нашу жизнь. Уже никого не удивишь доступом в Интернет, в который можно выйти практически из любой точки мира, несмотря на то, что буквально 20-30 лет назад это казалось чем-то невероятным.

Информационные технологии развиваются очень быстро и их развитие, безусловно, внесло очевидное удобство в жизнь людей: появилась возможность быстро передавать информацию на большие расстояния, использование интернет - телефонии упростило общение, стало реально мгновенно осуществлять денежные платежи и переводы.

Несмотря на бесспорные плюсы, трудно не обратить внимание на отрицательные стороны развития информационных технологий. Гаджеты, без которых, казалось бы, невозможно прожить и дня, несут в себя большую опасность. Не для кого не секрет, что они негативно влияют на здоровье человека. Кроме этого, через них возможно нанести удар и по вашим личным данным в социальных сетях, банковским счетам, а также узнать любую интересующую мошенников информацию о вас. В наш XXI век, мошенники больше не похожи на Остапа Бендера, но и у них есть 400 способов отъема денег. В наши дни способы интернет – мошенничества стали разнообразнее и более изощрённые. Одним из видов мошенничества является фишинг, о котором собственно и пойдет речь.

Актуальность и цель работы

Темой моего исследования является «Как защитить себя от фишинга». Эта тема очень актуальна и важна, так как в наше время - время информационных технологий, трудно найти человека, который не использует банковскую карту, в целях оплаты покупок через Интернет, и иных целях, связанных с Сетью, поэтому очень высока вероятность стать жертвой

интернет – мошенников на просторах Интернета. У меня возник интерес узнать, угрожает ли фишинг обучающимся и сотрудникам Седельниковского агропромышленного техникума и выявить среди них потенциальных жертв интернет – мошенников.

Объект исследования: фишинг, как основной вид интернет-мошенничества.

Предмет исследования: защита от фишинга.

Цель: Выявить оптимальные варианты защиты от фишинга и с помощью разработанного сайта помочь обучающимся и сотрудникам Седельниковского агропромышленного техникума не стать жертвами интернет - мошенников.

Задачи:

1) определить, что такое фишинг и как он появился в сети Интернет;
2) раскрыть все существующие способы защиты от фишинга;
3) разработать сайт для помощи в защите от фишинга.

Гипотеза: материалы сайта «Осторожно, фишинг!» помогут уберечь обучающихся и сотрудников Седельниковского агропромышленного техникума не стать жертвами интернет - мошенников.

Методы, используемые для реализации задач:

- социологический опрос
- сравнительный анализ
- поисковый
- систематизаций
- классификация

Тип проекта: исследовательский

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Историческая справка

Фишинг, как термин, появился в сети в 1996 году. Действия фишеров относились к компании «America Online», пользуясь именем которой мошенники получали доступ к аккаунтам ее абонентов. Полученные данные применялись для рассылки спама.

Более серьезные последствия фишинга встревожили сеть в 2001 году, когда атаке подверглись некоторые платежные системы, в частностие-gold. В результате работы злоумышленников, была собрана огромная база налогоплательщиков, содержащая их банковские реквизиты.

После всплеска популярности социальных сетей, фишеры расширили свои интересы и в этом направлении. В 2006 году была атакована известная зарубежная сеть MySpace, а в 2008 от злоумышленников досталось сети ВКонтакте.

По итогам анализа специалистов «Лаборатории Касперского» выяснилось, что за период 2012-2013 гг. ежедневно фишинговым атакам подвергалось 102,1 тысячи пользователей по всему миру, а это почти вдвое больше, чем за аналогичный предыдущий период. Лидерами по росту числа атакованных пользователей оказались 4 страны: Вьетнам, США, Индия и Германия – здесь этот показатель увеличился более чем на 100%.Большинство серверов, на которых размещались фишинговые страницы, были зарегистрированы на территориях США, Великобритании, Германии, России и Индии. А более половины (57%) всех идентифицированных уникальных источников атак располагаются на территории всего 10 стран. При этом количество этих самых источников атак за период с 2012 по 2013 гг. выросло более чем в 3 раза.

Согласно статистике «Лаборатории Касперского», в 2019 году в мире значительно выросло число пользователей, атакованных программами для кражи паролей, — на 72%. Всего продукты компании отразили подобные атаки на устройствах почти двух миллионов пользователей. Программы для кражи паролей

умеют извлекать информацию напрямую из браузеров. Это могут быть в том числе логины и пароли к различным аккаунтам, сохранённые данные платёжных карт и содержимое форм для автозаполнения.

Кроме того, в 2019 году значительно выросло число фишинговых атак, в ходе которых злоумышленники, как правило, пытаются заполучить личные и платёжные данные пользователей. В этот период решения «Лаборатории Касперского» ежемесячно предотвращали в среднем 38 миллионов попыток перехода пользователей на мошеннические сайты. Фишеры пристально следят за новостной повесткой и используют интерес широкой публики к разным крупным событиям и знаменитостям, придумывая официально выглядящие приманки и хитростью вынуждая человека нажать на вредоносную ссылку или оставить личные данные.

Что такое «фишинг»

Некоторые российские статисты утверждают, что страх перед мошенничеством с банковскими картами, в настоящее время, превосходит страх перед террористами. Специалисты в области Интернет-преступлений выделяют несколько видов мошенничества, самым основным и успешным из которых является фишинг.

Анализ работ Алексея Гладкий, «Мошенничество в Интернет. Методы удаленного выманивания денег» и Лэнс Джеймса, «Фишинг. Техника компьютерных преступлений», а также источники википедии позволили мне сформулировать максимально точное определение фишинга. Фишинг, от английского – рыбалка, подразумевает под собой примерно такой же способ поведения злоумышленников. Они бросают в сеть интернет «наживку» в виде фальшивых сайтов и ждут, когда вы, пребывая в твердой уверенности, что попали на оригинальный ресурс, введете в нужно месте свои логин и пароль.

Фишинг (англ. phishing, от *fishing* — рыбная ловля, выуживание и *password* — пароль) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи

паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Фишинговые сайты, как правило, живут недолго (в среднем — 5 дней). Так как анти-фишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счету. Но не все фишеры сами обналичивают счета жертв. Дело в том, что обналичивание счетов сложно осуществить практически, к тому же человека, который занимается обналичиванием, легче засечь и привлечь мошенников к ответственности. Поэтому, добыв персональные данные, некоторые фишеры продают их другим

мошенникам, у которых, в свою очередь, есть отработанные схемы снятия денег со счетов.

Технологии фишеров

Технологии фишеров совершенствуются. Так, появилось сопряженное с фишингом понятие — фарминг. Это тоже мошенничество, ставящее целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опасней, так как заметить подделку практически невозможно.

Наиболее популярные фишерские мишени — аукцион Ebay и платежная система PayPal. Также страдают различные банки по всему миру. Атаки фишеров бывают случайными и целевыми. В первом случае атака производится «наобум». Атакуются наиболее крупные и популярные объекты — такие как аукцион Ebay — так как вероятность того, что случайный получатель имеет там учетную запись, довольно высока. Во втором случае мошенники узнают, каким именно банком, платежной системой, провайдером, сайтом пользуется адресат. Этот способ более сложен и затратен для фишеров, зато больше шансов, что жертва купится на провокацию.

Воровство конфиденциальных данных — не единственная опасность, поджидающая пользователя при нажатии на фишерскую ссылку. Зачастую, следуя по ней, можно получить программу-шпиона, кейлоггер или троян. Так что если даже у вас нет счета, которым мошенники могли бы воспользоваться, нельзя чувствовать себя в полной безопасности.

Согласно данным Gartner, в США в 2006 году ущерб, нанесенный одной жертве фишинга, в среднем составил 1244 долларов США. В 2005 году эта сумма не превышала 257 долларов, что свидетельствует о невероятном успехе фишеров. В России ситуация несколько иная. Из-за того, что у нас электронные платежные системы пока не столь распространены, как на Западе, ущерб от фишинга не столь велик. Но с распространением в России электронных платежных систем

доля фишинга в общем почтовом потоке возрастет, и, соответственно, возрастет и ущерб от него. Так что, хотя данная проблема в России не стоит еще столь остро, готовиться к ней надо уже сейчас.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. И хотя на многих сайтах, требующих конфиденциальной информации, опубликованы специальные предупреждения о том, что они никогда не просят сообщать свои конфиденциальные данные в письмах, пользователи продолжают слать свои пароли мошенникам. Поэтому несколько лет назад была создана Anti-Phishing Working Group (APWG) — группа по борьбе с фишингом, в которую входят как компании-«мишени» фишеров, так и компании, разрабатывающие анти-фишинговый/анти-спамерский софт. В рамках деятельности APWG проводятся ознакомительные мероприятия для пользователей, также члены APWG информируют друг друга о новых фишерских сайтах и угрозах. Сейчас APWG насчитывает более 2500 участников, среди которых есть крупнейшие мировые банки и ведущие IT-компании. Так что, по оптимистическим прогнозам, через некоторое время пользователи научатся остерегаться фишерских сайтов, как в свое время научились с опаской относиться к письмам с вложениями от неизвестных адресатов. Пока же основной защитой от фишинга остаются спам-фильтры.

Примеры схем интернет-фишинга

Рассылка поддельных сообщений электронной почты, с просьбой подтвердить логин и пароль. Злоумышленники могут заспамить сообщениями миллионы адресов электронной почты в течение нескольких часов. Для этого базы предварительно покупаются. Однако за такие действия предусмотрена уголовная ответственность, а серверы, с которых рассылается спам, вычисляют и банят, поэтому этот способ медленно уходит в прошлое;

Мошенники создают электронные письма с поддельной строкой “Mail From:”, используя недостатки в почтовом протоколе SMTP. Когда посетитель

отвечает на фишинговое сообщение, письмо с ответом автоматически пересылается мошенникам по электронной почте;

Фишинговые схемы популярны при проведении интернет-аукционов. При этом товары выставляются на продажу через легальный интернет-аукцион, однако средства перечисляются через поддельный веб-узел;

Фиктивные благотворительные организации, обращающиеся с просьбой о пожертвованиях;

Создание фишинговых интернет-магазинов. Товары продаются по бросовым ценам либо с большими скидками. Это привлекает посетителей и они предоставляют данные своих банковских карт, не подозревая, что становятся жертвой мошенничества.

Разновидности фишинга

Сегодня можно выделить несколько основных видов фишинга: почтовый, онлайновый и комбинированный.

Первый вид подразумевает рассылку различных электронных сообщений. В них могут быть вложены «черви» или вирусы. Злоумышленники часто используют технологии, которые позволяют обходить спам-фильры, которые сегодня не гарантируют полноценную защиту. Кроме этого, получаемые сообщения могут принимать официальный вид и сбивать с толку получателей. Как уже упоминалось, может использоваться так называемая поддельная адресная строка.

Второй вид – онлайновый фишинг заключается в том, что мошенники достаточно качественно копируют наиболее популярные ресурсы (к примеру, интернет-магазины). Следующие шаги можно легко просчитать. Покупатель заходит на такую поддельную страничку и совершает покупку. При этом деньги уходят на счет мошенника.

Третий вид – комбинированный фишинг. Он сочетает в себе особенности двух вышеперечисленных способов обмана.

Наиболее частые жертвы фишинга

Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби-сети.

Характерной особенностью фишинговых писем является очень высокое качество подделки. Адресат получает письмо с логотипами банка / сайта / провайдера, выглядящее в точности так же, как настоящее. Ничего не подозревающий пользователь переходит по ссыке «Перейти на сайт и залогиниться», но попадает на самом деле не на официальный сайт, а на фишерский его аналог, выполненный с высочайшей точностью.

Еще одной хитростью фишеров являются ссылки, очень похожие на URL оригинальных сайтов. Ведь достаточно наблюдательный пользователь может обратить внимание на то, что в командной строке браузера высвечивается ссылка, совершенно отличная от легитимного сайта. Такие «левые» ссылки тоже встречаются, но рассчитаны они на менее искушенного пользователя. Часто они начинаются с IP-адреса, хотя известно, что настоящие солидные компании давно не используют подобные ссылки.

Поэтому фишинговые URL часто похожи на настоящие. Они могут включать в себя название настоящего URL, дополненное другими словами (например, вместо www.examplebank.com стоит www.login-examplebank.com). Также в последнее время популярный фишинговый прием — ссылка с точками вместо слешей, внешне очень похожая на настоящую (вместо www.examplebank.com/personal/login стоит www.examplebank.com.personal.login). Можно привести еще такой фишерский вариант: www.examplebank.com-personal.login.

Также в самом теле письма может высвечиваться ссылка на легитимный сайт, но реальный URL, на который она ссылается, будет другим. Бдительность пользователя притупляется еще тем, что в письме может быть несколько

второстепенных ссылок, ведущих на официальный сайт, но основная ссылка, по которой пользователю надо пройти и залогиниться, ведет на сайт мошенников.

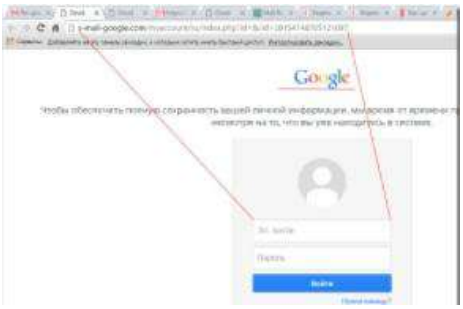
Иногда личные данные предлагается ввести прямо в письме. Надо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.

Защита от фишинга

Чтоб не стать жертвой мошенников необходимо вводить свои данные только на проверенных сайтах. Используйте расширения, защищающие пароли, и относитесь с опаской к заманчивым предложениям.

Рассмотрим правила, помогающие обнаружить поддельный сайт и избежать кражи ваших данных:

- Во-первых, тщательно проверяйте сайты, на которых вы работаете, особенно это касается сайтов банковских систем. Они должны иметь домены .ru .com Если указано .zz .org – стоит насторожиться. Также фишинговый сайт может иметь искажение адреса, например s-google.com. На это тоже стоит обращать внимание.



- Во-вторых, смотрите на дизайн сайта. Сайтам с устаревшим дизайном не следует доверять. Злоумышленники могут скопировать дизайн сайта, для присвоения данных для входа на него.

- В-третьих, обращайте внимание на соединение с сайтом. В строке с адресом должно быть указан протокол HTTPS. Многие браузеры оснащены функцией предупреждения о небезопасных сайтах. Внимательно читайте их.
- В-четвёртых, при оплате в интернет-магазинах проверяйте, что вас перенаправляет на официальный сайт вашего банка. В строке адреса появляется название организации и сведения о сайте.

Для защиты от фишинга достаточно установить антивирус. В них предусмотрено расширение, защищающее пароли по умолчанию. Антивирусы, имеющие встроенную web-защиту, автоматически блокируют нежелательные сайты.

Все популярные браузеры, имеют свою систему защиты, которая блокирует нежелательные сайты и сообщает пользователю, что велик риск кражи персональных данных.

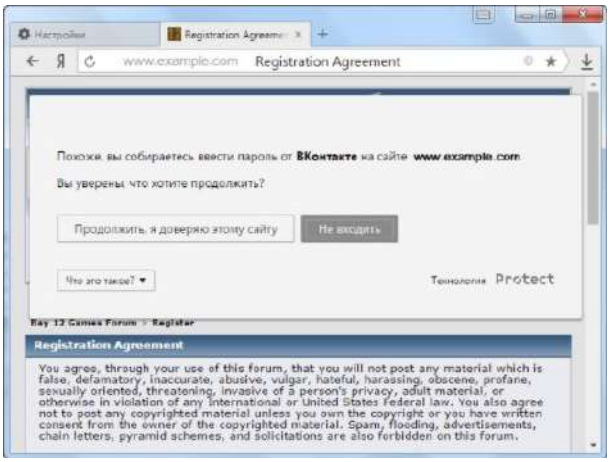
Защита от фишинга в браузере

Рассмотрим на примере защиту от фишинга в Яндекс Браузере.

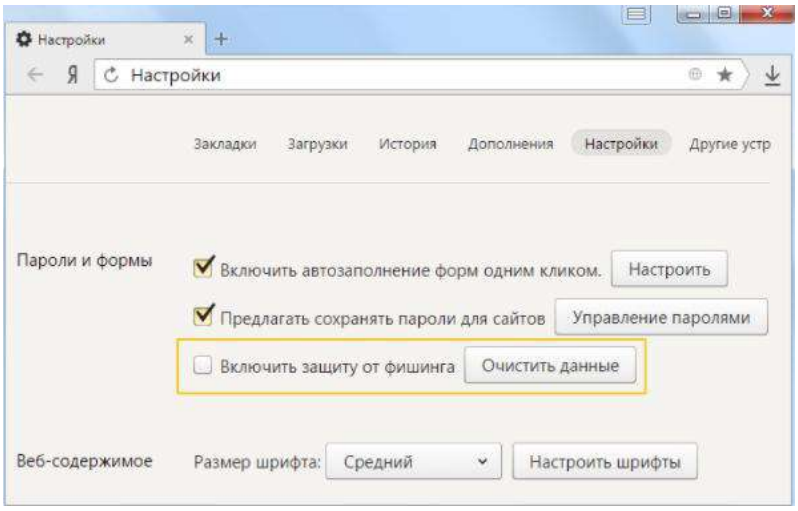
Этот браузер использует защиту паролей от фишинга, преобразуя его в отпечаток, так называемый хэш, и сохраняет в защищённой базе данных. Хэш представляет собой последовательность полученную после криптографического хэширования. Для примера слово «hello» будет выглядеть вот так: «2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824»

Хэш нужен лишь для сравнивания отпечатков паролей, и сами пароли не хранит. Даже если злоумышленники украдут базу паролей, расшифровать хэш они не смогут и, следовательно, не получат доступа к вашим файлам. Когда вы вводите пароль, он сравнивается с хэшем в базе, и если он совпадает с хэшем пароля от другого сайта, перед тем, как отправить пароль на сайт, браузер

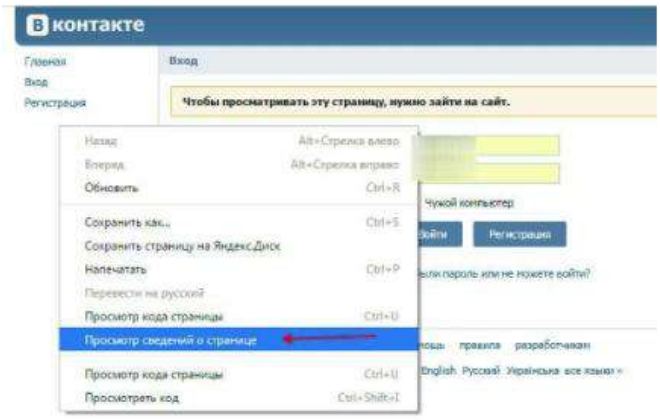
попросит подтвердить использование одного пароля на разных сайтах.



Для включения защиты от фишинга зайдите в настройки браузера и поставьте галочку в соответствующем поле.



У любого сайта можно проверить его состояние и настроить параметры защиты индивидуально. Для этого кликните правой кнопкой мыши в любой области сайта и нажмите «Просмотр сведений о странице», далее откроется окно, в котором будет показана безопасность соединения и меню выбора параметра защиты.



Программы для защиты от фишинга

Помимо встроенных утилит для защиты и шифрования могут быть использованы сторонние программы, защищающие ваши пароли.

Такими программами являются все антивирусы. Просто включите данную опцию в настройках вашего антивируса.

Инвайты и фишинг

Инвайты – это приглашения в интернете, необходимые для регистрации на закрытых ресурсах или скачивания файлов с ограниченным доступом.

Здесь тоже нужно быть осторожным. Мошенники, узнав, что вы запросили инвайт на закрытый ресурс, могут попытаться выслать вам поддельное приглашение на фишинговый сайт.

Для получения инвайт кода обращайтесь непосредственно к пользователям или администраторам сайта. Не соглашайтесь на покупку инвайтов со сторонних сайтов. При получении приглашения напишите администрации и узнайте, действительно ли код принадлежит этому сайту.

С учётом огромного их многообразия защититься от мобильных фишинговых атак значительно сложнее. Но и здесь будут уместны рекомендации, которые мы приводим для компаний, желающих защититься от компрометации деловой переписки, целевых атак и других видов мошенничества с использованием электронной почты.

1. Повышение грамотности пользователей в сфере безопасности: они должны знать об опасностях, которые несёт бездумное использование мобильных устройств, в частности, переход по ссылкам в сообщениях и установка программ из непроверенных источников. А если речь идёт об устройствах, используемых в рамках BYOD в трудовой деятельности, от установки приложений, не нужных для работы, лучше вообще воздержаться.

2. Тренировка навыков безопасного поведения: для этого следует обратиться к компаниям, которые предоставляют услуги имитированных фишинговых атак, и выяснить, есть ли в перечне их услуг тренировка противостояния мобильному мошенничеству.

3. Установка защитных решений на мобильные устройства: из перечня продуктов Trend Micro можно выделить приложения Mobile Security & Antivirus и Enterprise Mobile Security для Android и iOS, а также приложение Trend Micro WiFi Protection для защиты при работе в публичных беспроводных сетях.

ПРОЕКТНОЕ РЕШЕНИЕ

Перед началом исследования я предположил, что фишинг не угрожает обучающимся по сравнению с сотрудниками техникума. Это связано, по моему мнению, с тем, что обучающиеся являются активными пользователями сети и находятся в курсе многих уловок мошенников. Сотрудники, в свою очередь, являются более подверженными фишинг-атакам, так как мало знакомы с современными средствами общения, а они, как уже говорилось, несут в себе большую опасность. Так же, люди старшего поколения, имеют некоторые финансовые накопления на своих банковских счетах, которые в основном превышают накопления обучающихся, что делает их более интересными для фишеров, ведь одна из основных целей фишинга ¬ получение денежных средств.

Хочу обратить внимание на интересный факт, который для меня оказался неожиданностью: несмотря на то, что обучающиеся не являются потенциальными жертвами, но по разговорам большинство из них, считают, что им угрожают действия интернет ¬ мошенников.

С помощью различных источников в сети Интернет я нашел оптимальные варианты защиты от фишинга и решил с помощью разработанного сайта «Осторожно, фишинг!» помочь обучающимся и сотрудникам Седельниковского агропромышленного техникума не стать жертвами интернет - мошенников.

Рассмотрев широкий выбор конструкторов, я остановился на онлайн-сервисе от Google. Конечно, сервис от поисковика не может встать рядом с самостоятельными CMS платформами. Но у него есть ряд преимуществ:

- Создать сайт можно быстро.
- Без оплаты услуг веб-студий и фрилансеров.
- Без навыков и опыта работы в области конструирования веб-ресурсов.

“Google сайты” легкая в освоение платформа для создания сайтов. Ей легко могут воспользоваться как учителя, так и учащиеся. Google сайты можно использовать не только как платформа для веб сайтов, но и например как информационная доска и многое другое.

Определились с платформой для создания сайта, осталось разобраться с его контентом. На страницах сайта посетители смогут познакомиться с актуальным на сегодняшний день информационным преступлением – фишингом. А также проанализировать существующие сегодня проблемы выявления, устранения, профилактики таких преступлений и определить, какие существуют способы борьбы с киберпреступностью, в частности, с фишингом.

Сайт содержит разделы:

1. Что такое фишинг
2. Примеры фишинга
3. Разновидности фишинга
4. Защита от фишинга
5. последние новости о фишинге
6. Проверь себя

В последнем разделе собран полезный материал для проверки своих знаний.

1. Проверьте себя: насколько легко вас обмануть? В тесте собраны примеры как фишинговых, так и настоящих писем и сайтов. Попробуйте угадать, какие из них являются фейковыми, а какие – настоящими.

2. Фишинг или нет? Проверьте, способны ли вы вычислить интернет-мошенника. Необходимо ответить на 10 вопросов и узнать, легко ли вы ведётесь на уловки злоумышленников.

3. Фишинг или нормальное письмо из банка? Тест на финансовую грамотность (и еще на внимательность).

Работа над сайтом будет продолжена, так как в последнее время на фоне постоянных новостей о коронавирусе активизировались мошенники, которые используют актуальную повестку в корыстных целях.

Заключение

Не попадаться на обманы в интернете, на самом деле, очень просто, достаточно уметь думать, не доверять неизвестным людям, не заходить по не проверенным ссылкам, иметь хороший антивирус, регулярно проверять компьютер на наличие вирусов, и ни в коем случае не переводить деньги или давать часть своего имущества другим неизвестным пользователям, потому что его, в отличии от аккаунта уже не вернуть.

Считаю необходимым сказать, что соблюдение нескольких рекомендаций сохранит Ваши деньги в целости и сохранности:

1. Никогда не переходите по ссылкам от незнакомцев, будьте внимательны к тому, от кого пришла ссылка и куда она вас привела;

2. Не вводите свои логин и пароль, если у вас есть хотя бы малейшее подозрение, что сайт ведёт себя странно.

3. Регистрируясь на сомнительных сайтах со слабой защитой, используйте временный адрес и пароль. Почта — это ваш ключ ко всем аккаунтам – к ней нужен

4. отдельный, надёжный пароль.

5. Установите хорошую антивирусную программу.

6. Никому не сообщайте логин и пароль для входа в платежную систему банка.

Надеюсь, что материалы сайта «Осторожно, фишинг!» помогут уберечь обучающихся и сотрудников Седельниковского агропромышленного техникума не стать жертвами интернет - мошенников.

Список источников информации

1. Лэнс Джеймс, «Фишинг. Техника компьютерных преступлений», НТ Пресс, 2008 – 253 с.
2. Вехов В.Б., «Компьютерные преступления. способы совершения методики расследования», М., 2006. ¬ 182 с.
3. Алексей Гладкий, «Мошенничество в Интернет. Методы удаленного выманивания денег», М., 2012. – 102 с.
4. Романов Сергей, «Мошенничество в России. 1000 способов, как уберечься от фишинг¬атак», ЭКСМО¬Пресс, 2014 – 187 с. 8

Интернет источники:

Википедия https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3#%D0%98%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F

Компания Malwarebytes https://ru.malwarebytes.com/phishing/

Лаборатории Касперского https://www.kaspersky.ru/about/press-releases/2020_pochti-dva-milliona-polzovatelei-bili-atakovani-programmami-dlya-krazhi-parolei-v-2019-godu

Сбербанк- кибербезопасность https://www.sberbank.ru/ru/person/dist_services/cybersecurity

Семантик Диджитал https://semantica.in/blog/fishing.html

Сообщество ИТ-специалистов https://habr.com/ru/company/trendmicro/blog/473794/

Энциклопедия Касперского https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/