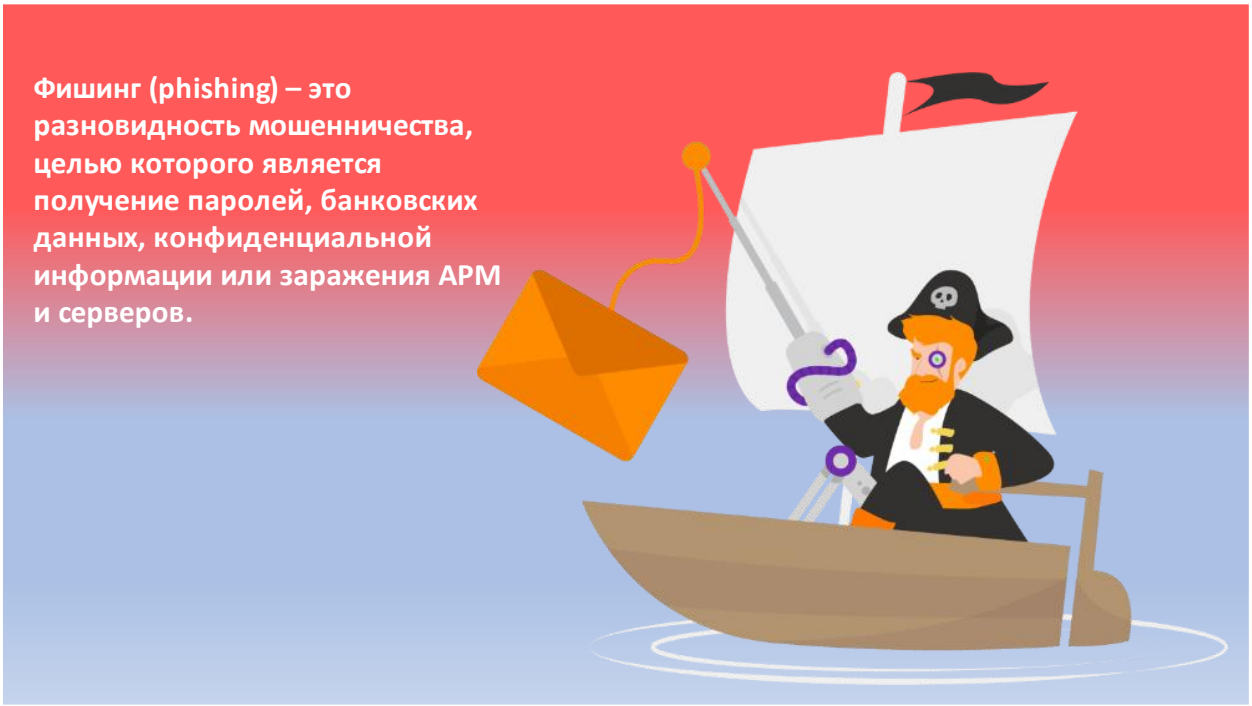


Фишинг (phishing) – это разновидность мошенничества, целью которого является получение паролей, банковских данных, конфиденциальной информации или заражения АРМ и серверов.

Техника фишинга была подробно ***описана еще в 1987 году***, а сам ***термин*** появился ***только в 1996 году***. Первой известной попыткой стала атака на платёжную систему e-gold в июне 2001 года, второй стала атака, прошедшая вскоре после теракта 11 сентября. Эти первые попытки были ***лишь экспериментом***, ***проверкой возможностей***. А уже в 2004 году фишинг стал наибольшей опасностью для компаний, и с тех пор он постоянно развивается и наращивает потенциал.

Как правило, злоумышленники массово рассылают электронные письма содержащие вредоносные вложения или ссылки на поддельные сайты новостных агентств, социальных сетей, банков или государственных органов. Также возможны варианты массовых мошеннических рассылок СМС или автоматических голосовых вызовов.

С фишинга начинается большинство современных кибератак. Пользователей корпоративных информационных систем, хотят обмануть, заставив запустить какой-то вредоносный файл или перейти на поддельный сайт. Поэтому несмотря на применяемые в организации меры по защите информации в определенных ситуациях ***именно от пользователей и их действий зависит*** – будет ли атака успешной и произойдет ли заражение.

Разновидности фишинга

1. Почтовый фишинг
2. Spear Phishing (спеарфишингили целевой фишинг)
3. Whaling (уэйлинг)
4. Smishing (смишинг)
5. Vishing (вишинг)
6. Business Email Compromise (компрометация корпоративной электронной почты)
7. Clone Phishing (клон-фишинг)
8. Фишинг в социальных сетях
9. Фишинг в поисковых системах
10. Pharming (фарминг)

1. Почтовый фишинг

Самый распространенный тип фишинга, злоумышленники выдают себя за некую легитимную личность или организацию, отправляя массовые электронные письма на все имеющиеся у них адреса электронной почты.

Такие письма содержат характер срочности, например, сообщая получателю, что его личный счет был взломан, а потому он должен немедленно ответить. Их цель заключается в том, чтобы своей срочностью ***вызвать необдуманное, но определенное действие от жертвы***, например, нажать на вредоносную ссылку, которая ведет на поддельную страницу авторизации. Там, введя свои регистрационные данные, жертва, к сожалению, фактически передает свою личную информацию прямо в руки мошенника.

2. Spear Phishing (спеарфишинг или целевой фишинг)

Вместо того чтобы использовать технику «spray and pray», как описано выше, ***спеарфишинг*** включает в себя отправку вредоносных электронных писем конкретным лицам внутри организации. Вместо того, чтобы рассылать массовые электронные письма тысячам получателей, этот метод нацелен на определенных сотрудников в специально выбранных компаниях. Такие типы писем часто более персонализированы, они заставляют жертву поверить в то, что у них есть отношения с отправителем.

Пример спеарфишинга

Armorblox сообщила о спеарфишинговой атаке в сентябре 2019 года против руководителя компании, компания которого была названа одной из 50 лучших инновационных компаний в мире. Письмо содержало вложение, которое, было внутренним финансовым отчетом, для доступа к которому требовалось пройти авторизацию на поддельной странице входа в Microsoft Office 365. На поддельной странице входа в систему уже было заранее введено имя пользователя руководителя, что еще больше усиливало маскировку мошеннической веб-страницы.

3. Whaling (уэйлинг)

Whaling (уэйлинг) очень похож на spear phishing (спеарфишинг), но вместо того, чтобы преследовать любого сотрудника в компании, мошенники специально нацеливаются на руководителей. К таким относятся генеральный директор, финансовый руководитель или любой другой высшего уровня, потому что как правило они имеют более широкие права доступа к конфиденциальным данным.

Пример уэйлинга

В ноябре 2020 года уэйлинг-атаке подвергся соучредитель австралийского хедж-фонда Levitas Capital. Соучредитель получил электронное письмо, содержащее поддельную ссылку в Zoom, которая внедрила вредоносное ПО в корпоративную сеть и почти привела к уводу 9 миллионов долларов на счета мошенников. В конечном счете злоумышленник смог заполучить только 800 000 долларов, однако последовавший за этим репутационный ущерб привел к потере крупнейшего клиента хедж-фонда, что вынудило его закрыться навсегда.

4. Smishing (смишинг)

smishing (смишинг) или SMS-фишинг. Принцип действия такой же, как и при осуществлении фишинговых атак по электронной почте: злоумышленник отправляет текстовое сообщение от, казалось бы, легитимного отправителя (например, заслуживающего доверия компании), которое содержит вредоносную ссылку.

5. Vishing (вишинг)

Vishing (вишинг), иначе известный как voice phishing (голосовой фишинг), похож на смишинг в том, что телефон используется в качестве средства для атаки, но вместо того, чтобы использовать текстовые сообщения, атака проводится с помощью телефонного звонка. Вишинг-звонок часто передает автоматическое голосовое сообщение (например, ваш банк или государственное учреждение).

Злоумышленники могут заявить, что вы задолжали большую сумму денег, срок действия вашей автостраховки истек или ваша кредитная карта имеет подозрительную активность, которую необходимо немедленно исправить, естественно предоставив необходимые им данные.

Пример вишинга

В сентябре 2020 года медицинская организация Spectrum Health System сообщила о вишинг-атаке, в рамках которой пациенты получали телефонные звонки от лиц, маскирующихся под ее сотрудников. Злоумышленники использовали такие меры, как лесть и даже угрозы, чтобы заставить жертв передать свои данные, деньги или доступ к их личным устройствам.

6. Business Email Compromise (компрометация корпоративной электронной почты)

Это форма фишинга, при которой злоумышленник получает доступ к учетной записи электронной почты высокопоставленного руководителя (например, генерального директора). Имея в своем распоряжении скомпрометированный аккаунт, кибер-преступник, выдавая себя за генерального директора, отправляет электронные письма сотрудникам организации с целью осуществить мошеннический банковский перевод или провести ряд других незаконных действий.

Пример CEO-мошенничества

Бухгалтер австрийской аэрокосмической компании FACC в 2019 году получил письмо якобы от генерального директора. В письме содержалась информация о требуемом финансировании

нового проекта, и бухгалтер неосознанно перевел 61 миллион долларов на мошеннические иностранные счета.

7. Clone Phishing (клон-фишинг)

Этот метод фишинга работает путем создания вредоносной копии недавно полученного сообщения от легитимного отправителя, которое якобы направляется повторно от, казалось бы, этого же отправителя. Любые ссылки или вложения из исходного письма заменяются вредоносными. Злоумышленники обычно используют предлог повторной отправки сообщения из-за того, что в первоначальном письме были указаны неверные ссылки или вложения.

8. Фишинг в социальных сетях

Фишинг в социальных сетях подразумевает использование VK, Facebook, Instagram и Twitter, чтобы получить конфиденциальные данные жертв или заманить их нажать на определенные вредоносные ссылки. Мошенники могут создавать поддельные аккаунты, выдавая себя за кого-то из знакомых жертвы, чтобы заманить ее в свою ловушку, или они могут даже выдавать себя за аккаунт службы обслуживания клиентов известной компании.

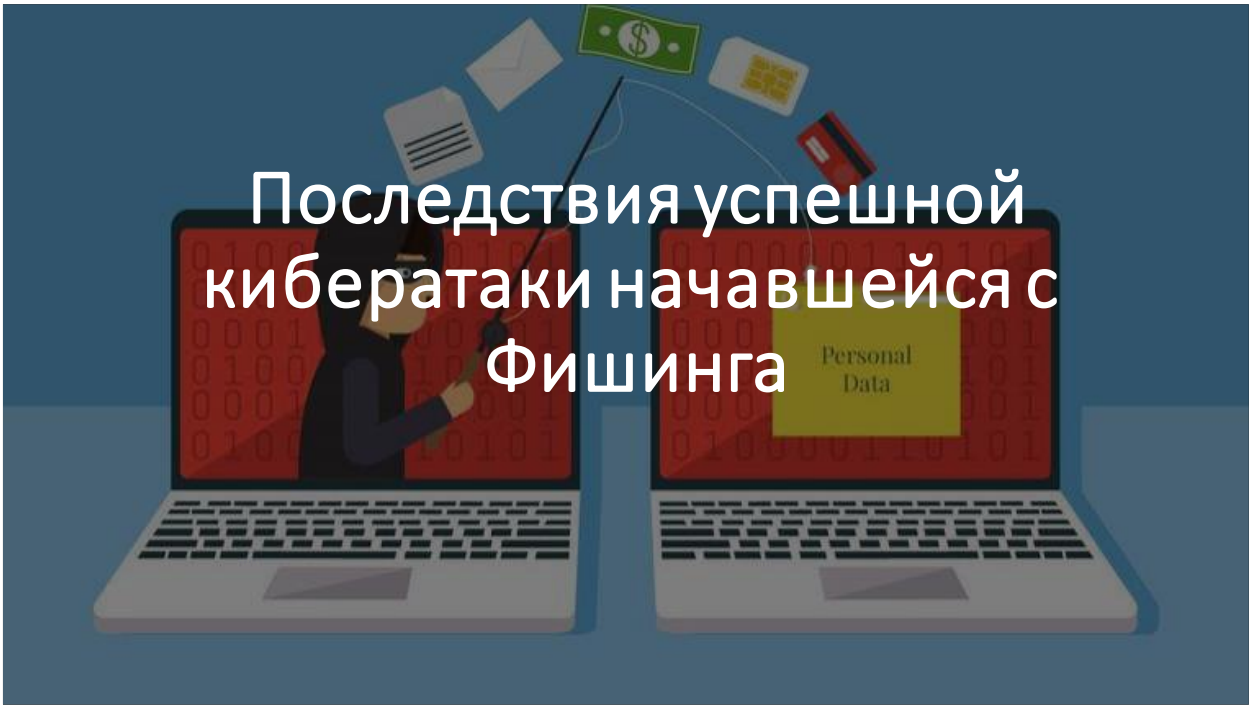
9. Фишинг в поисковых системах

При использовании фишинга в поисковых системах мошенники создают свой собственный веб-сайт и индексируют его в поисковых системах. Эти сайты часто предлагают дешевые товары и невероятно заманчивые предложения, пытающиеся заманить ничего не подозревающих онлайн-покупателей, которые видят сайт на странице результатов поиска в Google, Yandex или в других поисковиках. Если жертва нажимает в поисковике на ссылку для перехода на такой сайт, то, как правило, предлагается зарегистрировать аккаунт или ввести информацию о своем банковском счете для завершения покупки. Конечно, мошенники затем крадут эти личные данные, чтобы использовать их для извлечения финансовой выгоды в дальнейшем.

В 2020 году Google сообщила, что каждую минуту в поисковых системах появляются три новых фишинговых сайта!

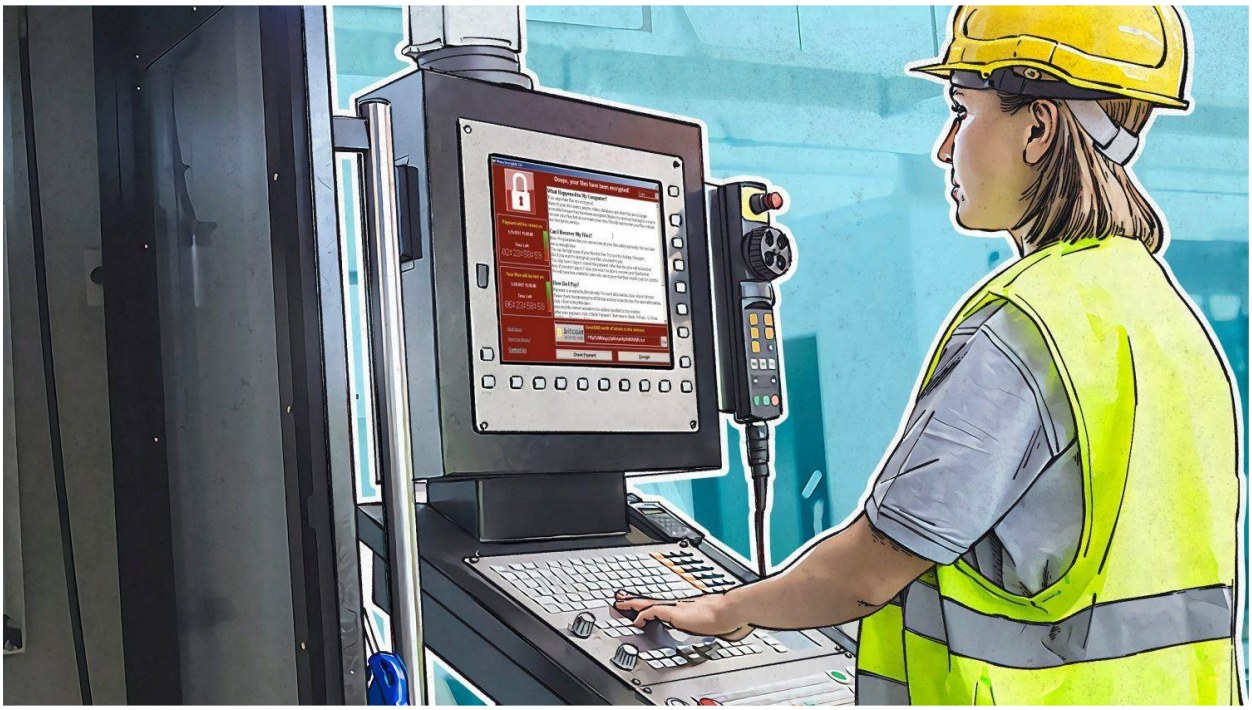
10. Pharming (фарминг)

Pharming (фарминг). В рамках данного типа фишинга мошенники, нацеливаясь на DNS-серверы (серверы доменных имен), перенаправляют пользователей, которые пытаются открыть какие-нибудь легитимные сайты, на вредоносные веб-сайты.



Последствия успешной кибератаки начавшейся с Фишинга.

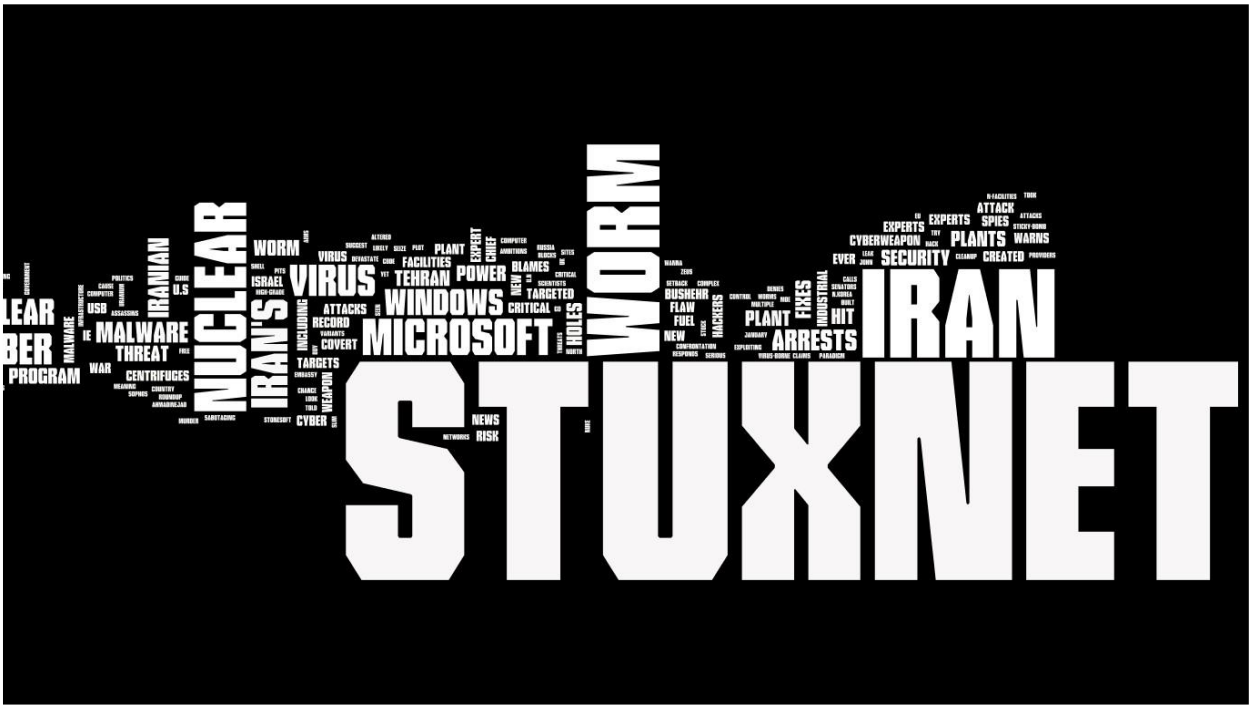
Надо помнить, что в случае заражения корпоративного компьютера вредоносным кодом оно может длительное время похищать ценную информацию оставаясь незамеченным. В дальнейшем утечка этой информации может нанести значительный ущерб для репутации и бизнеса организации.



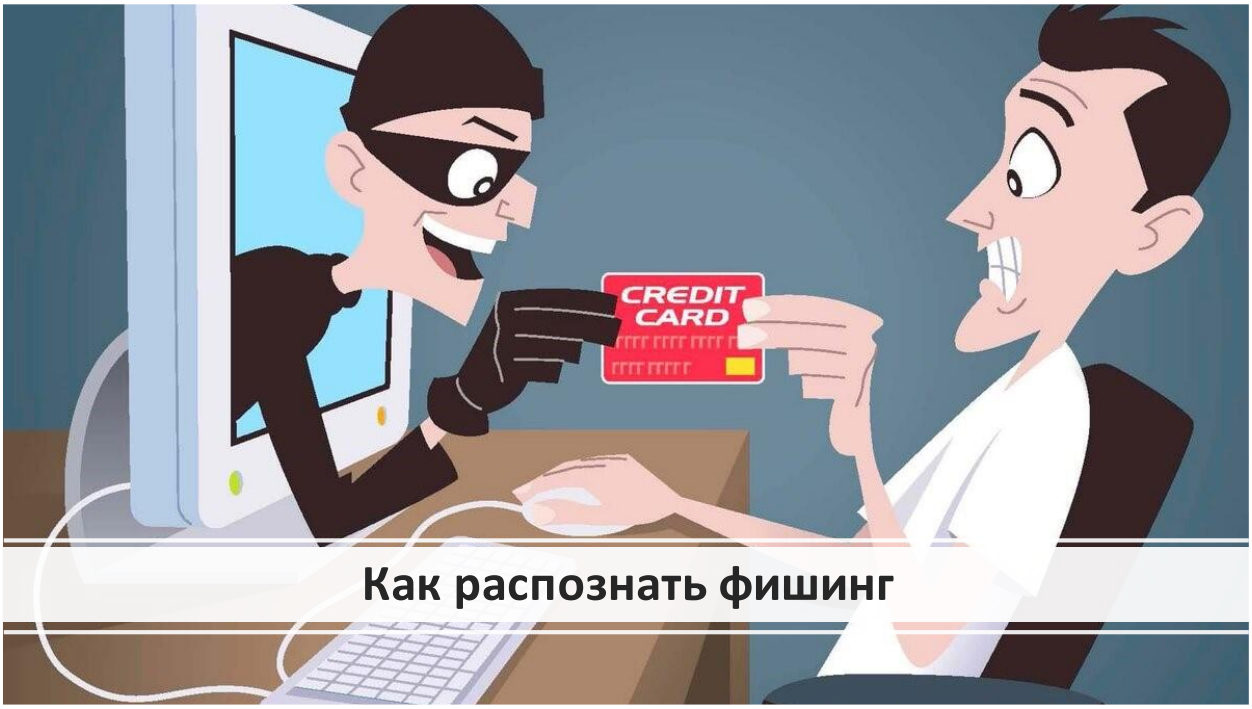
В 2017 году наиболее опасными оказались эпидемии вирусов шифровальщиков, таких как WannaCry и NotPetya, большая часть заражений которых пришлась на Российскую Федерацию.

В результате запуска вредоносного кода вся доступная информация на компьютере и сетевых папках оказывается зашифрованной и заблокированной. За расшифровку и восстановление доступа к файлам требуют достаточно внушительную сумму выкупа. При этом для многих пользователей и организаций информация оказывается безвозвратно потерянной.

Так же 2017 года из-за внушительного роста курса криптовалют, таких как bitcoin, существенное распространение получило вредоносное программное обеспечение, которые скрытно от пользователя и организации выполняет сложные вычисления, связанные с криптовалютами (майнинг). В результате этого существенно повышаются расходы на электроэнергию, а из-за сильной загрузки ресурсов компьютера, затрудняется работа в приложениях, необходимых пользователю для выполнения его служебных обязанностей.



В сентябре 2010 года в Иране около 30 тыс. компьютерных систем промышленных объектов были заражены вирусом Stuxnet. **Взлом привел к остановке работы более 1,3 тыс. центрифуг по обогащению урана в Натанзе** и переносу сроков запуска АЭС "Бушер". По словам экспертов, кибератака отбросила ядерную программу страны на два года. Власти Ирана обвинили во взломе спецслужбы США.



Как распознать фишинг

Фишинговые ссылки могут поступать через все каналы: социальные сети, личный и рабочий e-mail, мессенджеры, SMS, а также чаты и подобные ресурсы.

Обязательно нужно проверять URL-адрес, на наличие незначительных ошибок в написании.

Важно не переходить по коротким ссылкам вида bit.ly или goo.gl, даже если они приходят от друзей.

Использовать безопасные https-соединения. Отсутствие всего одной буквы "s" в адресе сайта обязано насторожить.

С подозрением относиться к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса, это не дает гарантии безопасности: он мог быть взломан или отправлен с подменой отправителя.

Получив неожиданное подозрительное сообщение, стоит связаться с отправителем каким-либо альтернативным способом и уточнить, он ли его послал.

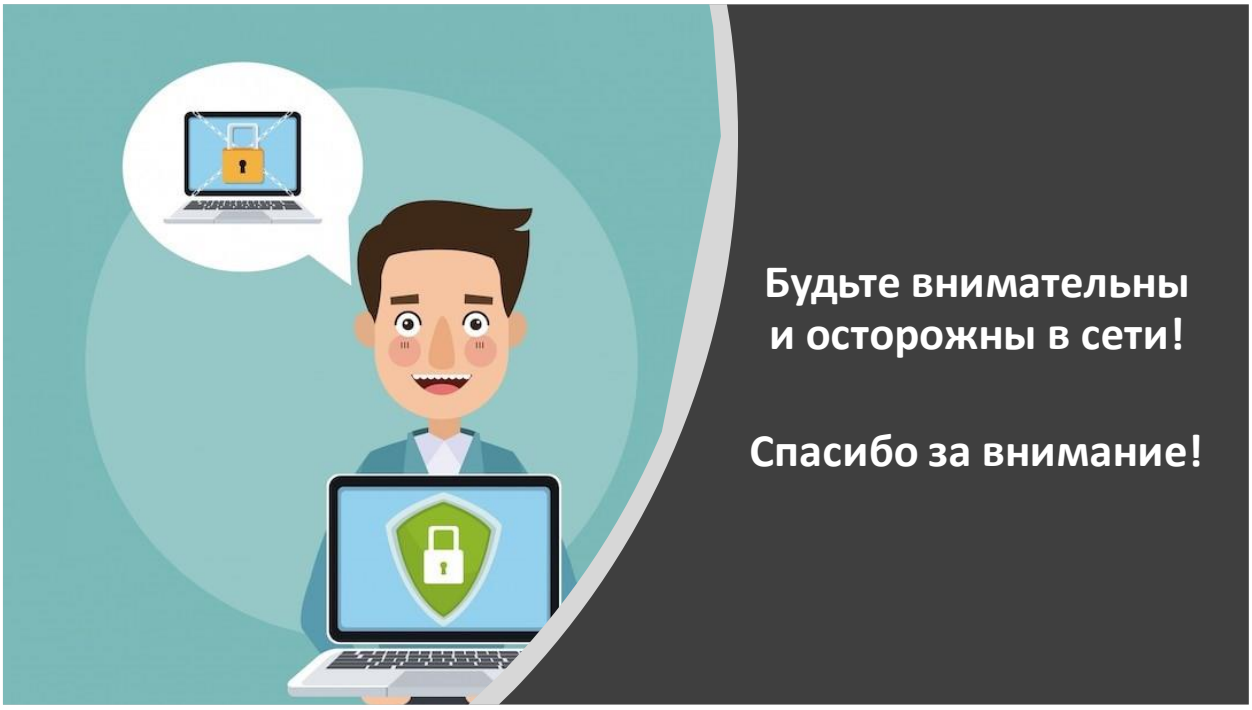
Если все же необходимо посетить ресурс, лучше ввести его адрес вручную или воспользоваться ранее сохраненными закладками (увы, от фарминга это не убережет).

Так же крайне не рекомендуется использовать для доступа к онлайн-банкингу и другим финансовым сервисам открытые Wi-Fi сети: часто их создают злоумышленники. Даже если это не так, подключиться к незащищенному соединению не составляет сложности для хакеров.

То же самое касается VPN сервисов, в особенности бесплатных, хотя и платные грешат этим.

На всех аккаунтах, где это возможно, подключить двухфакторную аутентификацию. Эта мера может спасти положение, если основной пароль стал известен взломщикам.

С помощью сервисов Whois, например на сайтах доменных регистраторов или сервисов на подобии 2IP.ru можно скопировать данные из адресной строки и узнать дату регистрации домена и данные владельца. Если дата регистрации свежая, то это повод задуматься о действиях мошенников. Крупные компании не регистрируют домены на частные лица, а используют данные юридического лица.



Будьте внимательны и осторожны в сети!

Спасибо за внимание!