RU

SAC 028
Рекомендации SSAC относительно противодействия фишинговым атакам по имитации регистраторов

ПРИМЕЧАНИЯ К ПЕРЕВОДАМ

Исходная версия данного документа на английском языке доступна по адресу http://www.icann.org/committees/security/sac028.pdf. Если существуют противоречия в переводе или заметные различия между данным документом и исходным текстом, исходная версия имеет приоритетное значение.

Рекомендации Консультативного комитета по вопросам безопасности и стабильности (SSAC) ICANN
май 2008 г.

Предисловие

В данных Рекомендациях описывается вариант фишинговой атаки, направленной на владельцев регистрации доменных имен. Злоумышленник выдает себя за регистратора доменных имен и отправляет клиенту (владельцу регистрации) ожидаемое или прогнозируемое сообщение относительно доменного имени. Примером ожидаемого сообщения может быть уведомление о скором истечении срока регистрации доменного имени, рекламное сообщение, уведомление, в котором владельцу регистрации сообщается о проблеме, связанной с управлением учетной записью, или любое другое сообщение, требующее непосредственного участия клиента либо предполагающее его. Однако это сообщение является поддельным. Фишер создает веб-сайт, похожий на сайт регистратора, чтобы убедить клиента войти в собственную учетную запись управления доменом и непреднамеренно сообщить свои учетные данные фишеру. Фишер использует полученные учетные данные клиента для доступа к портфелю доменных имен клиента, изменения сведений DNS о доменных именах в этой учетной записи и использования доменов для последующих атак.

В этих Рекомендациях SSAC описывает основные виды подобных атак. Мы рассмотрим типы и форматы сведений, включаемых в законные сообщения, которые регистраторы отправляют по электронной почте своим клиентам. Мы также обсудим, каким образом фишеры манипулируют этими видами и форматами сведений, создавая поддельные письма, предназначенные для того, чтобы с помощью *социального инжиниринга*[1] спровоцировать клиента регистратора посетить поддельный веб-сайт регистратора. Злоумышленник создает имитирующий веб-сайт таким образом, чтобы ввести клиента в заблуждение и убедить его выдать имена и данные учетной записи управления доменом. Мы обсудим некоторые из действий, рекомендуемых на данный момент для уменьшения количества или предотвращения фишинговых атак, направленных против финансовых учреждений и больших корпораций, которые обычно подвергаются подобным атакам. Также порекомендуем меры, которые следует предпринять регистраторам для уменьшения вероятности фишинговой атаки их корреспонденции с владельцами регистрации и определения способов, с помощью которых владельцы регистрации могут обнаружить попытку фишинга и избежать угрозы.

[1] См. статью «Почему фишинг работает», http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, содержащую дополнительные сведения о социальном инжиниринге.

Введение. Анализ атаки

Фишеры используют многие формы сообщений электронной почты, отправляемых торговыми или финансовыми организациями своим клиентам[2]. Регистраторы также используют электронную почту для многих видов корреспонденции, связанной с регистрацией доменных имен, включая следующие сообщения:

- сообщения о необходимости возобновления доменных имен;
- подтверждения заказа доменных имен;
- подтверждения запросов на регистрацию;
- подтверждения изменений сведений о доменах;
- напоминания о точности данных «кто есть кто»;
- уведомления об истечении срока действия или аннулировании регистрации доменных имен;
- предложения, рекламные сообщения о (новых) услугах и функциях.

Фишеры пользуются тем, что регистраторы полагаются на переписку по электронной почте. Имитируя (путем спуфинга) регистратора при фишинговой атаке, фишер может заманить клиента регистратора на поддельную копию страницы входа, на которой клиент, не сознавая этого, может предоставить учетные данные злоумышленнику. Эти учетные данные предоставляют фишеру несанкционированный доступ к учетной записи управления доменным именем. Учетная запись содержит различные ресурсы, полезные для злоумышленника:

- регистрации доменов клиента, которые могут быть изменены в целях злоумышленника (см. «Перспектива угрозы»);
- (потенциально) возможность использования кредитных карт или других способов оплаты, доступных через записи регистратора, с помощью которых могут приобретаться дополнительные домены для последующего использования в целях злоумышленника.

Для осуществления атаки по имитации регистратора фишеры собирают сведения из нескольких источников. Фишер копирует страницы, изображения, эмблемы и файлы, необходимые для создания реалистичной, но поддельной копии страницы входа регистратора, с «настоящего» веб-сайта регистратора. Они помещаются на веб-сервер, управляемый фишером, и используются для спуфинга страницы входа регистратора. Фишер также использует сведения, полученные из типовых сообщений регистратора клиентам, чтобы «персонализировать» обращение, включаемое в фишинговое сообщение электронной почты. Получить такие сообщения можно, просто став владельцем регистрации у того регистратора, на которого планируется атака. Фишер использует сведения «кто есть кто» для еще большей степени персонализации фишинговых сообщений; что более важно, фишер может воспользоваться сведениями «кто есть кто» для составления списка получателей, которые являются владельцами регистрации у регистратора, на которого планируется атака.

[2] Примеры отчетов о фишинге и мошенничестве можно найти в архиве фишинга органихации Anti-Phishing Working Group (http://www.apwg.org/phishing_archive/phishing_archive.html) and MillersMiles.co.uk (http://www.millersmiles.co.uk/archives.php).

Использование сведений, полученных из сообщений регистратора

Некоторые регистраторы могут включать в типичные сообщения электронной почты сведения, связанные с регистрацией доменного имени. К ним могут относиться имя (идентификация личности) и счет клиента, номера финансовых документов и квитанций. Некоторые регистраторы включают в сообщения контактную информацию и сведения о службе поддержки клиентов, в том числе телефонные номера, адреса электронной почты и URL-адреса (гиперссылки). Некоторые регистраторы, использующие сообщения электронной почты на основе HTML, включают в них эмблемы компании, рекламные баннеры и изображения «брендов».

Злоумышленники могут воспользоваться тем, что регистраторы включают в сообщения эти сведения, при создании фишинговых сообщений электронной почты для клиентов таких регистраторов. Например, фишер может включить номера личного счета клиента и номера финансовых документов, чтобы *персонализировать* сообщение, как показано в следующем примере общей части гипотетического фишингового сообщения электронной почты в текстовом формате:

```
БЛАГОДАРИМ ЗА ВАШ ЗАКАЗ
Среда, 19 октября 2005 г., 5:18:34

Уважаемый клиент,

Благодарим Вас за использование услуг <регистратора>. Ниже
приведены подробные сведения о вашем последнем заказе. Пожалуйста,
сохраните эти сведения для последующего использования.

НОМЕР КЛИЕНТА: 123456789
ИМЯ ВХОДА: blablablalalala
НОМЕР КВИТАНЦИИ: 298884-3340
СУММА: $19.99
ТЕЛЕФОН СЛУЖБЫ ПОДДЕРЖКИ: 800-555-1234

Чтобы завершить эту операцию, необходимо выполнить вход в вашу
учетную запись. Пожалуйста, перейдите по следующей ссылке для
подтверждения: http://www.<регистратор>.tld/login
```

В этой гипотетической атаке URL-адрес `http://www.регистратор.tld/login` в действительности является помещенной в сообщение электронной почты гиперссылкой, которая перенаправляет жертву атаки на другой сервер, например, тег HTML, обрамляющий в сообщении электронной почты текст `http://www.регистратор.tld/login`, может выглядеть следующим образом:

```
<a
href="http://кражадоменаэтимспособом.tld">http://www.регистратор.tld/login</a>
```

При выборе этой ссылки будет выполнен переход на страницу `кражадоменаэтимспособом.tld`. Включение сведений о клиенте не всегда необходимо для фишинговой атаки, сведения также не обязательно должны быть полностью точными. Однако включение даже неверных номеров учетной записи или финансовых документов повышает достоверность обмана: сообщение *выглядит* настоящим, и хотя некоторые клиенты могут сохранять подробные сведения о транзакциях и помнят номера клиентов, другие не делают этого, и такие клиенты могут принять любой номер (или личные данные) за настоящий без проверки. Кроме того, неточные сведения могут обеспечить ответ от владельца регистрации, который в противном случае проигнорировал бы сообщение. Рассмотрим воображаемого владельца регистрации, Джона Смита, который дорожит доменным именем `smith.tld`. Он получает напоминание о точности данных «кто есть кто», которое содержит контактную информацию для другого лица с той же фамилией, как показано в гипотетическом напоминании о точности данных «кто есть кто» ниже:

```
От: whoisreminders@whoisupdate.com
Время отправки: среда, 12 декабря 2007 г., 11:57
Кому: Джон Смит
Тема: Напоминание о данных «кто есть кто»

Уважаемый клиент,

В соответствии с резолюцией 03.41 о Политике относительно
напоминаний о данных «кто есть кто» (WDRP) Корпорации Интернета по
распределению имен и адресов мы напоминаем Вам, что общедоступную
контактную информацию «кто есть кто», связанную с регистрацией
Вашего доменного имени, следует постоянно обновлять. В наших
записях от 15 ноября 2007 года содержится следующая информация.

Доменное имя: smith.tld
Дата регистрации: 9 августа 2006
Дата истечения срока регистрации: 9 августа 2008
Контактная информация владельца регистрации
Имя: Питер Смит
Адрес: ул. Смита, д. 11
Адрес: (нет)
Город: Смитвилль
Штат/провинция: Пенсильвания
Почтовый индекс:
Страна: США
Сведения об административном контакте
Имя: Питер Смит
Адрес электронной почты: psmith@iamtherealsmith.tld
Адрес: ул. Смита, д. 11
Адрес:
Город: Смитвилль
Штат/Провинция: Пенсильвания
Почтовый индекс:
Страна: США
Номер телефона: 7305825074307
Имя регистратора: <регистратор>
Сведения о серверах доменных имен
```

```
Если какие-либо из приведенных выше сведений неточны, необходимо
исправить их,

посетив страницу http://исправитьмоисведенияwhois.tld/login[3].
Обратите внимание, что согласно условиям договора о регистрации
предоставление неверных сведений «кто есть кто» может быть
причиной для отмены
регистрации вашего доменного имени.
```

Опасаясь перехвата доменного имени, Джон быстро реагирует, чтобы исправить проблему. В спешке он выбирает вставленную в сообщение ссылку, переходит на фишинговый веб-сайт и передает свои учетные данные фишеру.

Использование информации, полученной из служб «кто есть кто»

При атаке по имитированию представителя регистратора используется следующая последовательность событий:

1. Фишер создает поддельный клиентский портал регистратора (сайт входа).
2. Фишер создает сообщение электронной почты, якобы отправленное регистратором.
3. Фишер отправляет это сообщение на контактные адреса электронной почты для заданного доменного имени (либо избирательно, то есть определенному владельцу регистрации, либо в рамках массовой фишинговой атаки клиентам регистратора, на которого ведется атака).
4. Некоторые из клиентов регистратора оказываются жертвами обмана, переходят на поддельный клиентский портал регистратора и выдают свои учетные данные входа.
5. Фишер получает учетные данные владельца регистрации для незаконного использования в дальнейшем.

Из этой последовательности событий ясно, что фишер должен сопоставить клиента, доменное имя и поддерживающего это доменное имя регистратора, чтобы попытаться осуществить атаку по имитации регистратора. Службы «кто есть кто» предоставляют сведения о регистрации доменного имени, включая имя и почтовые реквизиты владельца регистрации, адреса электронной почты административного и технического контактов домена, а также информацию о регистраторе, поддерживающем доменное имя. Типичный результат запроса службы «кто есть кто» приведен ниже.

```
Domain ID:D2347548-LROR
Domain Name:ICANN.ORG
Created On:14-Sep-1998 04:00:00 UTC
Last Updated On:16-Nov-2007 20:24:23 UTC
Expiration Date:07-Dec-2011 17:04:26 UTC
Sponsoring Registrar:Register.com Inc. (R71-LROR)
Status:DELETE PROHIBITED
Status:RENEW PROHIBITED
Status:TRANSFER PROHIBITED
```

[3] В этом примере внедренный в фишинговое сообщение электронной почты тег HTML содержит IP-адрес, а не доменное имя, например, <a "href=http://206.197.43.103/login/"> http://исправитьмоисведенияwhois.tld/login .

```
Status:UPDATE PROHIBITED
Registrant ID:C4128112-RCOM
Registrant Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Registrant Organization: Internet Corporation for Assigned Names and Numbers
Registrant Street1:4676 Admiralty Way, Suite 330
Registrant City:Marina del Rey
Registrant State/Province:CA
Registrant Postal Code:90292
Registrant Country:US
Registrant Phone:+1.3108239358
Registrant FAX:+1.3108238649
Registrant Email:icann@icann.org
Admin ID:C4128112-RCOM
Admin Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Admin Organization:Internet Corporation for Assigned Names and Numbers
(ICANN)
Admin Street1:4676 Admiralty Way, Suite 330
Admin City:Marina del Rey
Admin State/Province:CA
Admin Postal Code:90292
Admin Country:US
Admin Phone:+1.3108239358
Admin FAX:+1.3108238649
Admin Email:icann@icann.org
Tech ID:C1-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
Tech Street1:575 8th Avenue
Tech Street2:11th Floor
Tech City:New York
Tech State/Province:NY
Tech Postal Code:10018
Tech Country:US
Tech Phone:+1.9027492701
Tech FAX:+1.9027495429
Tech Email:domain-registrar@register.com
Name Server:NS.ICANN.ORG
Name Server:A.IANA-SERVERS.NET
Name Server:C.IANA-SERVERS.NET
Name Server:B.IANA-SERVERS.ORG
```

Во многих случаях регистратор или службы «кто есть кто» третьих сторон предоставляют дополнительные сведения о домене, включая такие данные:

- состояние безопасности (доступен ли сайт по SSL или HTTP);
- даты создания и последнего изменения доменной записи (в некоторых случаях может быть получена частичная или полная история домена);
- дата истечения срока действия записи о домене;
- состояние реестра (код состояния EPP[4], который назначен реестром для имени: clientTransferProhibited, RedemptionPeriod и т.п.);
- данные о сервере, например тип веб-сервера, (например, Apache, Microsoft IIS), состояние веб-сайта (например, активен), IP-адрес, состояние в черных списках;
- сведения DNS (имена и IP-адреса серверов имен);
- поиск по владельцу регистрации (например, поиск других доменов, зарегистрированных тем же владельцем регистрации);

[4] Протокол EPP (Extensible Provisioning Protocol), см. RFC 3731. http://www.rfc-archive.org/getrfc.php?rfc=3731

- ключевые слова META, используемые владельцем регистрации доменного имени для уточнения поиска;
- реклама.

Злоумышленники могут использовать сведения, полученные из ответов «кто есть кто», для массового фишинга владельцев регистрации или для избирательного фишинга владельцев регистрации, основанного на ожидаемых сообщениях, например о приближающемся истечении срока действия доменного имени. Определенные сведения «кто есть кто» содержат информацию о контактных данных владельцев доменных имен и, следовательно, о получателях сообщений электронной почты, а также о поддерживающем регистраторе, которого будет имитировать фишер (отправитель сообщения электронной почты). Другие сведения могут использоваться для повышения достоверности основной части сообщения; например даты создания, последнего изменения и истечения срока действия доменной записи могут использоваться для создания поддельного напоминания о возобновлении регистрации, данные о состоянии безопасности могут использоваться для создания поддельного уведомления о проблемах с SSL-сертификатом и т.д.

Перспектива угрозы

Перехват доменного имени с помощью фишинговой атаки такого вида возможен, но, как правило, не является основной целью злоумышленника. После того, как злоумышленник получает доступ к учетной записи владельца регистрации, он может изменить записи DNS через регистратора таким образом, чтобы они указывали на контролируемые злоумышленником сервера имен. Это обычная цель преступных и злоумышленных действий, при которых службы имен используются для атак fast flux[5]; когда адреса указывают на системы под контролем злоумышленника, он может манипулировать значениями «времени существования» (TTL) и изменять записи DNS данных доменной зоны на собственных серверах имен, расположенных по этим адресам.

Злоумышленник может использовать DNS не только для атак fast flux. Например, злоумышленник может добавить или изменить следующие записи в данных управляемой им доменной зоны.

- **MX**, чтобы выполнять перенаправление на почтовые хосты, контролируемые злоумышленником, и использовать их для рассылки спама. Использование домена владельца регистрации может быть предпочтительнее использования домена, который мог бы быть зарегистрирован злоумышленником напрямую, так как во многих случаях домен владельца регистрации является «доверенным» для других почтовых систем, то есть он не использовался как источник спама или не имеет репутации домена, рассылающего спам, он также не упоминается в черных списках, и получение писем от него не блокируется каким-либо образом.

- **A** или **AAAA**, чтобы выполнять перенаправление на системы, в которых размещаются поддельные веб-сайты, также управляемые злоумышленником (веб-сайты являются самыми популярными, но таким же образом могут изменяться IP-адреса FTP-серверов и других служб хостинга). Затем злоумышленник может размещать на поддельном сайте любое содержимое по своему усмотрению; например, злоумышленник может решить испортить веб-сайт и нанести ущерб имиджу владельца регистрации.

  Фишеры могут также заменять информацию на сайте на неверную, чтобы нарушить деятельность владельца регистрации. Примерами такой формы атаки могут быть объявления о значительных скидках, применяемых к ценам на продукты, об отзывах продуктов и т.д. Злоумышленник также может разместить выглядящие невинными гиперссылки, направляющие посетителей на сайты, на которых размещается опасное загружаемое содержимое, или которые подставляют опасное содержимое вместо изначально предполагавшихся приложений и исполняемых файлов.

[5] См. SAC022, *Атаки Fast Flux* и *DNS*, http://www.icann.org/committees/security/sac025.pdf

- **A** или **AAAA**, чтобы осуществлять перенаправление на системы, в которых размещаются поддельные внутренние или клиентские веб-сайты, также контролируемые злоумышленниками. Злоумышленник может выбрать целью атаки компанию, предоставляющую по Интернету доступ к конфиденциальной информации через страницу проверки подлинности. Если записи DNS перенаправляются на поддельную страницу проверки подлинности в интрасети, контролируемую злоумышленником, злоумышленник может рассчитывать, что обманутые, ничего не подозревающие сотрудники выдадут свои имена входа и пароли, которые могут быть проданы или использованы позднее в направленных атаках против этой компании. Финансовые учреждения являются основной целью таких атак, так как в этом случае раскрытие клиентами сведений о собственных учетных записях могло бы привести к мошенническим транзакциям и краже средств. Однако компании и организации, предоставляющие доступ к конфиденциальной, частной или личной информации, защищаемой нормами законодательства об охране конфиденциальной информации, также рискуют оказаться целью таких атак.

Этот список не является полным, а просто показывает, записи DNS каких типов изменяются или добавляются фишерами на сегодняшний день.

Добавление или изменение записей DNS

По-видимому, фишеры предпочитают добавлять записи DNS, а не заменять их, так как владелец регистрации может в течение более продолжительного времени не узнать об атаке, если все или некоторые из имен в его домене и далее разрешаются ожидаемым образом. Более того, за счет злоупотребления доменным именем, принадлежащим владельцу регистрации с хорошей деловой репутацией, злоумышленник может рассчитывать на сомнения после того, как организации, которые борются с фишингом или защищают торговую марку, объявят о злоупотреблениях. Регистраторы могут колебаться или отказаться предпринять меры против доверенного клиента, настаивать на получении судебного ордера и т.д., что может задержать приостановку любых незаконных действий, производимых в связи с определенным доменным именем.

Злоумышленник также может воспользоваться средствами администрирования домена, предоставляемыми регистратором, для включения перенаправления, или изменить домен таким образом, чтобы записи DNS указывали на другое расположение (ссылку). Если атакуемый фишером клиент регистратора использует услуги регистратора по хостингу веб-сайтов или электронной почты, злоумышленник может загружать и изменять содержимое на веб-сайте клиента, создавать учетные записи электронной почты (для спама), а также манипулировать существующими учетными записями в домене, изменять их и включать перенаправление.

Как регистраторы могут уменьшить степень угрозы фишинга

Помимо торговых и финансовых учреждений, фишеров также стали интересовать и поставщики услуг регистрации доменов. Регистраторы и посредники должны подтверждать, что они являются целью фишинговой атаки. SSAC рекомендует, чтобы регистраторы (и посредники) были очень внимательны и использовали лучшие методы защиты от фишинга при составлении писем к клиентам. Настоятельно рекомендуется использовать следующие методы.

1. Включайте в отправляемые письма только сведения, необходимые для передачи сообщения. Не включайте номера счетов клиента, личные данные и (в большинстве случаев) сведения о регистрации. Это позволяет фишерам персонализировать сообщения электронной почты.

2. Избегайте использования гиперссылок в переписке с клиентами. Фишеры в большинстве случаев маскируют ссылки, чтобы перенаправить пользователей с настоящих страниц на поддельные.

3. Предупредите клиентов, что не следует щелкать гиперссылки, как в текстовой форме, так и в виде изображений, которые могут содержаться в любых письмах. Включайте в основную часть рассылаемых вами сообщений такие предложения, как «для защиты от фишинга, пожалуйста, наберите следующий веб-адрес в строке адреса вашего веб-браузера» и «Не доверяйте ссылкам в сообщениях электронной почты. Всегда набирайте веб-адреса вручную в строке адреса веб-браузера». Многие клиенты оценят заботу об их безопасности и защите конфиденциальности, даже если ввод адреса вручную будет для них непривычным по сравнению с щелчком ссылки.

4. Повышайте уровень осведомленности о том, что регистраторы являются объектом фишинговых атак. Предоставляйте (или дополняйте существующие) страницы вопросов и ответов, чтобы привлечь внимание к фишинговым атакам по имитации регистраторов, опасности, которую представляют такие атаки, мерам, предпринимаемым вами для предотвращения фишинговых атак, и мерам, которые могут предпринять ваши клиенты, чтобы обнаружить такую атаку и не стать ее жертвой. Объясните, какие виды сведений вы будете включать в сообщения электронной почты, и, в особенности, определите сведения, которые вы *никогда* не будете помещать в свои сообщения, чтобы клиенты имели возможность определить, является ли полученное ими сообщение настоящим или подозрительным.

5. Обеспечьте для клиентов возможность сообщать о возможных фишинговых атаках, либо напрямую, либо посредством какой-либо организации, которая принимает образцы подозрительных мошеннических сообщений электронной почты и поддерживает репозиторий фишинговых сообщений электронной почты[6].

6. Рассмотрите возможность внедрения способов подтверждения авторства сообщений электронной почты для переписки с клиентами, например с помощью цифровой подписи.

[6] Страница сообщения о фишинге APWG по адресу http://www.antiphishing.org/report_phishing.html

Как владельцы регистрации могут избежать атаки по имитации регистратора

Владельцы регистрации несут ответственность за защиту собственных вложений в доменные имена. Эта ответственность не менее важна в контексте присутствия организаций в Интернете, ведения деятельности и бизнеса, чем ответственность по защите личных идентификационных данных от кражи и злоупотребления. Организации по защите потребителей, финансовые учреждения и компании-эмитенты кредитных карт предупреждают потребителей об опасности мошенничества в Интернете и объясняют, каким образом можно обнаружить фишинговую атаку и избежать ее. Многие из этих советов применимы и для избежания фишинговых атак по имитации регистратора. Некоторые из самых важных советов повторно приводятся ниже.

1. Не щелкайте гиперссылки, содержащиеся в полученных вами сообщениях электронной почты. Вместо этого вводите адреса веб-страниц вручную в строке адреса веб-браузера.

2. Используйте почтовый клиент с поддержкой функций защиты от спама и фишинга или установите хорошо зарекомендовавшее себя дополнение или подключаемый модуль, реализующий эти функции для вашего почтового клиента.

3. Используйте почтовый клиент, который может отображать адрес гиперссылки, связанной с видимым текстом или изображениями, содержащимися в сообщении электронной почты, или же ознакомьтесь со способами просмотра и прочтения «исходного» сообщения электронной почты в текстовом формате (ASCII). Научитесь читать теги гиперссылок, такие как HREF, чтобы быстро распознавать методы обмана, при которых отображается ссылка вида `www.пример.com`, но в действительности эта ссылка ведет к домену злоумышленника, например

   ```
   <A HREF="http://обманутебя.tld">www.пример.com</a>
   ```

   или по IP-адресу, например

   ```
   <A HREF="http://192.168.2.3">www.пример.com</a>.
   ```

4. Относитесь с подозрением к сообщениям электронной почты, в которых требуется немедленная реакция, а единственным вариантом действий является посещение веб-сайта. Большинство надежных компаний в Интернете, в том числе и регистраторы, предоставляют другие возможности связаться со службой клиентской поддержки, например по телефону, факсу или адресу электронной почты. Если вы не уверены, обратитесь к своему регистратору, используя альтернативные виды связи, особенно те, о которых вы узнали при личном посещении регистратора.

5. Внимательно читайте основную часть сообщения электронной почты. Грамматические ошибки и неправильная пунктуация часто указывают на то, что сообщение электронной почты является поддельным.

6. Не доверяйте сообщению электронной почты лишь потому, что оно является персонализированным.

7. Не вводите личные сведения или сведения об учетных записях в любых веб-формах предоставления сведений, пока не убедитесь, что находитесь на настоящей странице.

8. Всегда проверяйте, защищены ли посещаемые вами веб-формы предоставления сведений и страницы входа с помощью SSL. Однако гиперссылке не следует доверять лишь потому, что она, кажется, направляет на безопасную страницу. Проверьте подлинность цифрового сертификата, связанного с защищенными SSL страницами[7]

9. Если вы намерены оплатить услуги предоставления доменного имени с помощью кредитной карты, выберите регистратора, у которого клиенты должны вводить значение кода проверки карты (CVV) во время транзакции. Код CVV – это средство безопасности, которое компании-эмитенты кредитных карт используют, чтобы убедиться, что карта принадлежит вам, при покупке.

10. Передавайте сведения о сообщениях электронной почты, вызывающих подозрения в фишинге, своему регистратору или антифишинговым организациям, например в APWG, Phish Report Network[8], PhishTank[9] или местное отделение CERT[10].

Дополнительные сведения о защите от атак фишеров можно получить на страницах рекомендаций для потребителей, предоставляемых организациями Anti-Phishing Working Group[11], PhishTank и SpamHaus Project[12].

[7] См. SSL.com, вопрос Q10068 - FAQ: Как узнать, является ли веб-страница безопасной? http://info.ssl.com/Article.aspx?id=10068.
[8] Сеть сообщений о фишинге (Phish Report Network), http://www.phishreport.net/
[9] PhishTank: присоединяйтесь к борьбе с фишингом, http://www.phishtank.org
[10] Добавить здесь адреса электронной почты или веб-страниц.
[11] Совет потребителю. Как избежать фишингового мошенничества, http://www.antiphishing.org/consumer_recs.html
[12] Каталог вопросов и ответов по проекту SpamHaus (FAQ), http://www.spamhaus.org/faq/index.lasso

Заключение

В общем, доменные имена стали очень ценным товаром, а доменные имена, за долгое время существования заслужившие репутацию достойных доверия, являются основной целью злоумышленников. Имитация регистратора с целью получения учетных данных клиента и, таким образом, получения доступа к его регистрациям доменных имен является серьезной угрозой фишинга. SSAC рекомендует регистраторам и посредникам признать, что они являются целями фишинговых атак, и принять меры для предотвращения злоупотреблений.

SSAC признает, что фишинг процветает с помощью обмана и социального инжиниринга. Фишеры будут пытаться противодействовать мерам, предпринимаемым регистраторами. В конечном счете ответственность за защиту от мошенничества и обмана лежит на потребителях. Поэтому, хотя регистраторам доступны различные меры противодействия фишингу, самым важным является повышение уровня осведомленности клиентов и рекомендации клиентам с осторожностью отвечать на сообщения от регистратора.