Adam Alnak

October 24th 2016

# An overview of the public domain security systems of the PokerStars online platform

## Table of Contents

## 1. Background

Poker is the name given to a family of skill based card games which are based upon making bets. Each player will have a specific combination of cards, part of which will be unknown to opponents until the end of the hand. It is closely associated with other forms of gambling and historically took place in traditional brick-and-mortar casinos, as well as card rooms throughout the world.

The popularity of the game boomed in the early 21st century largely due to the emergence of online platforms for players and this has continued until the present.[i] The history of online poker is interesting from a security point of view. Falling under the gambling umbrella has meant it has often faced cultural and legislative stigma which means that its development has always been under immense scrutiny.[ii]

Poker differs from most forms of gambling in that the players are in a zero-sum game against each other, rather than the house. This fact more than any other means that even in a traditional, offline card game, the efficacy of information security is fundamental. If an opponent can find out your cards then the entire premise of the game is undermined.

Traditionally poker players have spent long periods of time sitting at cramped tables with strangers who were openly trying to take their money from them. For this reason, many players have a naturally wary disposition. The early years of online poker were littered with famous scandals[iii] which have affected the way the game is perceived. Black Friday[iv] involved several of the biggest online card rooms falling foul of US laws and led to online play being banned outright in that country.

The nature of the game means that it attracts a more numerate, and suspicious user base than a representative sample of the population. For this reason, online poker rooms face greater interest in things like security methodology from their customers than most online businesses would. Poker players are acutely aware that any flaw in their information security is going to directly affect their bank balance.

The points listed above were the motivation for this report.

*

PokerStars is the largest online poker cardroom in the world.[v] Today it is the central hub of the online poker community and hosts huge numbers of games in a variety of formats and in different variants of poker. It makes money primarily through tournament entry fees or a 'rake' - essentially for every bet placed in a poker hand PokerStars take a cut, much like the house in a real casino[vi].

It should be noted that poker games are accessed through PokerStars proprietary software which a user must download, rather than the website. This has far reaching implications for information security. PokerStars also operate account management options including payment systems through the https://www.pokerstarscasino.uk/ website.

This report intends to provide a high-level overview of some of the security issues that affect PokerStars and their customers. It will consider how sensitive customer data such as payment information is treated, and the measures in place to ensure game integrity. Privacy concerns are especially important because of the cultural stigma attached to gambling in some cultures and this will also be considered.

## 2. Risk Assessment

### *2.1 Assets and Systems*

This section will look at some of PokerStars' assets and their importance within the system. This report defines an asset as some knowledge or resource under the management of PokerStars.

Assets can be thought of as having a level of sensitivity and criticality. *Sensitivity* is a measure of the impact of the data being accessed by non-authorised parties, or if it is altered in any way. *Criticality* evaluates how dependent the system is upon an asset.

Table 1 considers the variety of security concerns for different assets. The consequences of failed security will be discussed in later sections of this report.

Figure 1 is a simple approximation of how the PokerStars system architecture is designed. It is intended as an aide to help visualise information being stored and transferred.

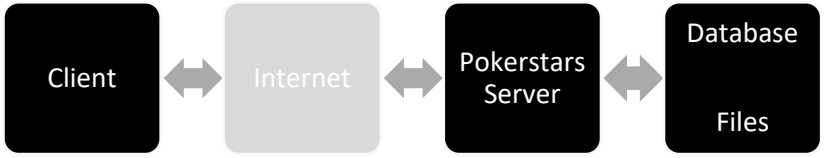


Fig 1: PokerStars system architecture

| ASSETS | SECURITY PROPERTIES |
|---|---|
| SERVERS AND NETWORKS (PHYSICAL ASSETS) | Fundamentally sensitive and critical. All data is stored or passed through the PokerStars servers and networks and these are central to the successful running of the site. If confidentiality or integrity are breached, then the fairness of games will be undermined. There are tight physical controls on access to servers (dedicated secure facility, zoned biometric access). Significant resources are spent ensuring hardware operates properly (constantly cooled server rooms, dedicated fibre-optic cables).[vii] |
| CODE AND METHODOLOGY (SOFTWARE ASSETS) | Highly sensitive and critical. While much of PokerStars methodology (e.g. for random number generation) is not confidential, it is vital for integrity that it cannot be altered in any way. Games cannot operate without successful application of the methodology. |
| CUSTOMER DATA: PERSONAL AND FINANCIAL, DATABASES (INFORMATION ASSETS) | Highly sensitive and somewhat critical. If the confidentiality of customer data is breached there are likely to be serious repercussions for the affected individuals. PokerStars will still be able to operate as before, however there are likely to be legislative and reputational consequences. |

Table 1: Security concerns of different assets. The table refers to the well-established CIA triad of security.[viii]

### *2.2 Risk Identification*

This section will consider the different types of threats faced by PokerStars. Possible vulnerabilities and exploits will be looked at and where possible some of the basic control measures will be tested in compliance with the assignment warning.

Threat sources can be roughly divided into 4 types: ADVERSARIAL, ACCIDENTAL, STRUCTURAL and ENVIRONMENTAL.[ix] This report will primarily focus on adversarial threats. This report defines a *vulnerability* as a potential way into a system and an exploit as a method that is developed to attack an asset by taking advantage of a vulnerability.[x]

As a business that facilitates online payments PokerStars deals with the usual threat actors: criminals and thieves, malicious insiders, online vandals. Being a poker site means there are some specific threats it faces on top of these. There are political considerations, with certain powerful groups dedicated to lobbying against online poker.[xi] The game of poker itself is of an adversarial nature as players compete against one another. This heightens the threat from users attempting to exploit vulnerabilities to gain an unfair advantage over their competitors. Table 2 (see Appendix) details some of these malicious parties and their motivations.

By far the most likely attack on a user will involve trying to obtain their data.[xii] The attack tree in Figure 2 shows various ways a threat actor could try to gain access. Each of these attacks has a degree of difficulty associated with it. "E" represents easy, "M" is moderate and "D" is difficult. This is a reflection on the resources required to launch the attack. If one method of attack is difficult, a threat actor is likely to switch their attention to an easier one. If successful security measures are put in place then a particular vulnerability may become unattractive to malicious parties looking to exploit it due to the change in the resource requirement.

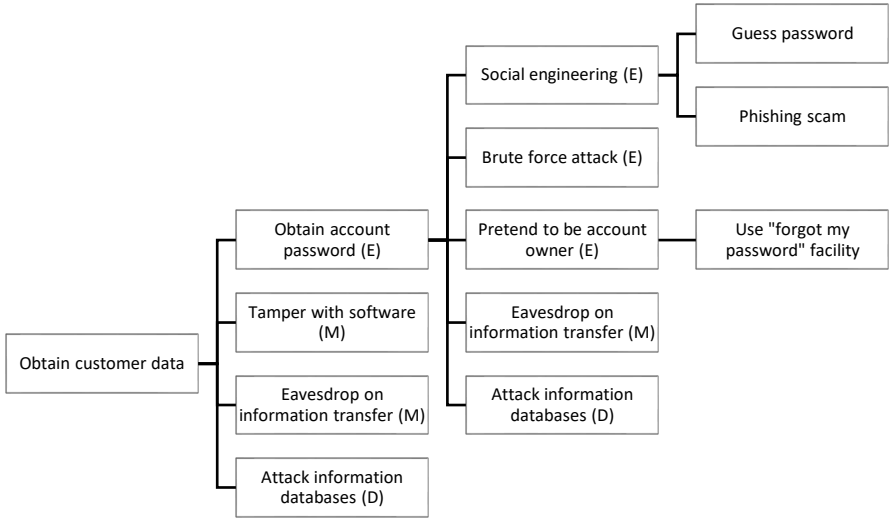


Fig 2: Ways a malicious actor could try to extract customer data

Attacks also have a likelihood of success. For example, while it requires almost no resources to try to guess a user's password, it is also unlikely to yield success. Even if it did, the data from only one customer would be gained. On the other hand, obtaining access to information databases would be extremely difficult. It would require intimate knowledge of the security systems in place, a great deal of time and sufficient technical skill. However, if these databases were obtained, the attacker would have a very high chance of successfully gaining access to vast amounts of customer data.

It should be noted that the attacker can either target the user or business systems directly. For a very large organisation such

as PokerStars with strong and established security measures in place, attacks on individual customers rather than the company itself can be much easier and require significantly less technical knowledge.

Figure 2 shows that one of the easiest routes to obtaining customer data is to obtain a user's password. The most basic attack on password security is simply to try to guess the password, for example by attempting to use common names or dates. A slightly more sophisticated version of this is a brute force attack where many possible passwords are tried until the correct one is found.

A particularly popular group of attacks are known as "social engineering". This refers to the manipulation of users to voluntarily divulge information. An example of social engineering is a phishing scam where legitimate users are sent emails from scammers purporting to be from PokerStars. These attacks are particularly dangerous because they have a very low resource requirement. A scammer can target hundreds of customers in one go, and only requires a small success rate to start stealing data or money. PokerStars users have been the victim of phishing scams in the past.[xiii]

Eavesdropping can be a more sophisticated route of attack than breaking password security. It refers the unauthorised interception of private information as it is being transferred between locations. An example would be rerouting traffic between the PokerStars servers and the web app that the customer is running. This would make the traffic which will include customer data visible to the attacker.

*

Online poker players rely on the premise that the game they are playing is fair. The sanctity of this principle can be considered another aspect of their online security which can be attacked.

PokerStars users therefore face the risk that the methodology used to generate the cards is flawed. For games to be fair they rely on random shuffling. This means that every possible combination of cards should have an equal likelihood of being generated. If there is a problem in the software cards can be generated unequally. If someone knows the flaws in the distribution, then they will be able to more accurately predict which cards are generated than the other players and will have an unfair advantage.

Some poker sites including PokerStars make their methodology public to reassure customers that they are secure. This is based on the principle of "no security through obscurity" – that is the idea that a system should remain secure even if all its components are known. Security should be based on sound mathematical principles rather than deception.[xiv] This is good practice, however making the system public does not guarantee that it is designed correctly. A random shuffle is harder to generate than it sounds. Potential flaws can be mathematically subtle and go unnoticed for long periods of time – and they can have devastating effects on the fairness of the game.[xv]

Finally, even if the methodology is perfect there is still a risk if there is a possibility that the software can be tampered with. This is particularly important to consider when software is being downloaded. Users must be sure that the software is from PokerStars and has not been modified in any way.

The countermeasures that PokerStars have in place to protect customer data will be discussed in the next section.

### *2.3 Identifying Vulnerabilities, Exploits and Countermeasures*

In order to look at some real vulnerabilities and exploits while maintaining compliance of the rules, some basic tests were made on password control strategies using my personal PokerStars account.

Considering the attack tree in Figure 2 I first I looked at allowable password parameters. Figure 3 (see Appendix) shows that PokerStars passwords must be at least 8 letters long and that they must begin with a letter. They must also be less than 26 characters long and contain a number. This means that users are not allowed to use the most basic passwords which makes guessing them harder. Assuming only alphanumeric characters are used there are $8^{62}$ possible 8 letter passwords. However, having restrictions on allowable password also reduces the possible combinations so there are much fewer possible 8 letter passwords than $8^{62}$. It is well within present computing capabilities to be able to guess such a small number of possibilities quickly which leads onto the next point.

PokerStars limits the number of login attempts allowed to 5. After this an error message is displayed and my account was frozen for some time. This is an effective countermeasure to brute force attacks.

The other elements of social engineering discussed in Table 2 are the "forgot password" function. When I selected this and entered my username, I received the email shown in Figure 4 to my registered account. This itself is a control measure since usernames are public but email addresses are not. This means the password reset function is only available if you can find the associated email account. However, there is a problem here in that you can enter your email address rather than your username at this stage which gives rise to a possible exploit –

Imagine a hacker has obtained access to hundreds of email addresses from another source unrelated to PokerStars. She may not know if any of them have a PokerStars account, but she can enter each of them into the forgot password function and if they do she will receive a link to reset the password. This is a shallow level of protection and means that PokerStars accounts are only as secure as the email account associated with them.

The password reset process generated the email in Figure 4 (see Appendix) which I have shown in full. This is relevant from a phishing point of view. The email has a simple layout and would be easy to replicate. Furthermore, the URL for the password reset is not obviously a PokerStars link (i.e. not pokerstars.com/*). Another possible exploit would therefore be for a threat actor to send out emails that look the same but redirects the reset password link to a third party which requires some customer data to be input. This technique would be especially effective if the attacker already had access to a list of PokerStars associated email accounts.

I believe the password control issues raised are real vulnerabilities despite the control measures in place.

With access to an account it is possible to obtain the following: username, email address, name, address, date of birth, partial payment information. It is also possible to make further deposits using any payment cards linked to the account without further verification. Unauthorised account access is therefore a serious breach of sensitive data.

*

Tampering with software, trying to eavesdrop on information transfer or attacking databases is far beyond the scope of this report. Fortunately, PokerStars provides some information about the security controls they have in place.[xvi]

Firstly, the installer executable file for PokerStars software is signed using an RSA 2048 bit certificate which ensures that the client has software which came from PokerStars and which has not been altered between publication and installation.

As stated in Table 1, servers are well physically secured. Countermeasures to protect against eavesdropping include the following (taken from PokerStars website):

- Our client software uses the certificates issued by our own Certificate Authority (CA) to authenticate our servers
- Our client software uses the industry standard TLS protocol. We are currently using a 2048-bit RSA key, which according to RSA is sufficient until 2030. As we review and update private server keys every three months, we are secure within a large safety margin. We support the following ciphers: AES128-SHA (128 bits) and DES-CBC3-SHA (168 bits).
- No private data, such as pocket cards, is ever transferred to other players (except in accordance with the game rules).
- All client input is validated server-side.

These countermeasures show that there is a good level of security in place to protect against the vulnerabilities. Encryption is to a good standard and exceeds basic cryptographic requirements for security. With sufficient time and resources no system is secure indefinitely. PokerStars have incorporated a good safety margin to ensure that they refresh their security standards as time passes and before they become exploitable.

*

To illustrate how a software flaw can fatally undermine a poker platform, consider briefly a real case from the early days of online poker. In 1999, PlanetPoker made the code they used to shuffle their cards publicly available in an attempt to prove its rigour. It was analysed by a group of poker players who also happened to be internet security professionals.

In a real deck of cards, there are 52 ! (approximately $2^{226}$) possible unique shuffles. The analysts knew the random number generator function used a seed based on the number of milliseconds since midnight per the system clock. There are only 86,400,000 milliseconds in a day and thus only 86,400,000 possible shuffles. By synchronizing their program with the system clock, they could reduce the number of possible combinations to a number on the order of 200,000 possibilities.

Given the fact that in Texas Hold'em poker 5 cards are known to each player after the first round, they created a program which searched through the few hundred thousand possible shuffles and deduced which was a perfect match. They then knew which players held what cards, what the rest of the cards to be dealt would be, and who was going to win in advance ![XV]

Just like in the case of PlanetPoker, PokerStars make their random number methodology public. They have taken sophisticated measures to ensure a fair shuffle which include[XVI]:

- using two independent sources of random data – user input including a summary of mouse movements, and Quantis which uses hardware to monitor and use quantum randomness as a source of entropy.
- 249 random bits (the number of possible shuffles is a 226 bit number) from both entropy sources are used to generate shuffles
- Independent verification of the random number generator to accepted industry standards by Gaming Laboratories International.

Online poker is much more sophisticated now than it was in 1999, and PokerStars have demonstrated appropriate commitment to ensuring fair poker games. This type of software problem can be considered to have a very low risk of affecting users.

*

Given the security countermeasures found in previous sections, it is plausible to imagine that PokerStars operate a whole raft of other controls which have not been discussed.

For example, it is likely that there are physical controls around server stores which could take the form of security patrols, security fences and electronic access monitoring. There are also probably controls to help reduce the risk of company employees unnecessarily accessing customer data such as never allowing staff to obtain unencrypted customer passwords and only required staff having access to data centres. A further area which has not been discussed is the potential use by attackers of malicious software to monitor players' screens while they play to see their cards. PokerStars software is likely to have some level of security built in to prohibit certain third party software running at the same time.

### *2.4 Determining Risk and Control Recommendations*

PokerStars operate in a relatively security conscious space. Throughout this report it has been apparent that the company take information security seriously and devote significant resources to protecting it. Having said this, there are still serious security risks it faces.

This section of the report refers to the threat-vulnerability pairs in Table 3 in the Appendix.

Unauthorised system access is the low-hanging fruit of information security. Attacks are easier to instigate and attackers can target individual customers to reduce the need to get around PokerStars' countermeasures. Row 2 of Table 3 describes the risk of unauthorised access through social engineering and phishing methods. Although the table states the risk as "low" due to the relatively small impact on critical PokerStars' processes in the event of individual data breaches, there is still evidence that reputational damage can ensue, particularly where multiple customers are affected. There are also concerns about PokerStars' processes not protecting users as much as they should. For example, it seems that there are limited or no system flags in place for users accessing the site from two geographically distant locations in quick succession; for repeated failed deposit attempts; or for withdrawal to new unidentified payment accounts.[xvii] These are relatively basic control measures that a large operation such as PokerStars should and could put in place very easily.

Worryingly, I also found some potential vulnerabilities in my basic tests. The number of "forgot my password" attempts should be limited at least by IP address, although this could be evaded using web proxies. Additional control measures such as security questions *in addition* to email account access should be required to protect customers whose email accounts have been compromised.

More should be done to reduce the likelihood of successful phishing attacks on users. This could include making official emails easier to identify and harder to forge. However even if controls are improved, this type of attack is still likely to persist. The risk should therefore be communicated better to users to improve awareness of the problem and to clearly state what PokerStars will and will not do in their official correspondence.

Another note was that user passwords must start with a letter. This seems unnecessary and reduces the number of possible passwords, which would make them easier to crack should the controls on the number of password attempt be circumvented. This restriction should be removed.

There are also many security control measures that users can implement themselves. The most important is choosing a strong password for their PokerStars account *as well as* the associated email account. PokerStars also allows for the enabling of two-factor authentication using an RSA Security Token. This means that access of the account is only possible if the user has both the password *and* a physical security token they must have with them. Two-factor authentication is a strong defence of account security and should be used when possible.

*

There are good control measures in place to reduce the risk of data interception. However, more risk could be avoided altogether by removing financial functions from the PokerStars website and bringing them all within the proprietary software which is easier to control.

Potential software flaws were discussed in the previous section and this report is satisfied that this risk has been sufficiently reduced by control measures to be acceptable. It is plausible that external parties such as Quantis have insurance in place to cover business interruption in the event of their systems failing. This may extend to PokerStars and is an example of how insurance could help deal with risk that cannot be eliminated.

The video referenced in Table 1 shows some of the countermeasures protecting servers and data centres from physical attack. Along with the controls mentioned in the previous section, these appear to be reflective of the risk and it is reasonable to accept the residual risk. Further action (that may already be in place) could include the division of data into multiple secure sites to reduce the amount of data compromised in a single breach.

*

Overall security controls are already to a good standard, and so it was surprising to find that the proposed improvements to password security which could be so easily implemented for such minimal cost have not been completed already. They should be prioritised as urgent.

Similarly, better flagging systems should be developed to provide protection for customers *after* their account has been breached. Simple measures such as limiting the number of allowed failed withdrawal attempts would be effective

against many online thieves. There would also be a reputational boost for PokerStars if these changes were effectively communicated.

The other suggestions vary in difficulty and can be considered as best practice rather than crucial.

PokerStars users can generally be satisfied that their account security is secure, so long as they themselves take reasonable care.

## 3 Critique

This report was limited by several significant factors: the technical capability of the author, legal considerations relating to looking for account data, and availability of information about PokerStars' processes.

There were also some limitations in the methodology used. To get a realistic impression of the threats faced by an organisation of the scale of PokerStars, Tables 2 and 3 would have had to be much larger. Qualitative risk was described in Table 3 and can be misleading in several ways. The classification system used (very low – low – medium – high – very high) is blunt and something of the true magnitude of risk can be lost. There is also the possibility that risk is classified at an unrepresentative level if care is not taken when considering the relationship of the likelihood and impact for specific cases. It would also be very difficult to forecast accurate numerical costs and probabilities for the threat-vulnerability pairs. There are so many variables involved, so many unknown unknowns as well as known unknowns, that using specific figures was prohibited

Overall the risk management strategies in this report work at a high level. They could flag some simple recommendations and improvements but, for a system as well-established and well-resourced as PokerStars, were unlikely to find any critical issues. A much more thorough, forensic analysis of risk would be able to provide more valuable recommendations and it is very likely that PokerStars already use such tools to monitor their risk strategies.

Ultimately, it was impossible to look at some parts of the PokerStars security system in detail because information is necessarily not public. This report was therefore only able to comment on specific security items and hypothesize about the rest.

END

[i] History of online poker - http://www.toppokersites.com/history-of-online-poker/
[ii] When will online poker be legal in my state? - http://redchippoker.com/when-will-online-poker-be-legal-in-my-state/
[iii] Absolute Poker Scandal 2007 - http://www.absolutepokerscandal.com/absolute-poker-scandal-2007
[iv] Black Friday five years later - https://www.pokernews.com/news/2016/04/black-friday-five-years-later-24506.htm
[v] http://www.pokerscout.com/
[vi] 'What is a rake?' - https://www.pokerstars.com/help/article/global/poker-rake-explanation/

[viii] "When I'm playing online where do the games take place?" - https://www.youtube.com/watch?v=Tvmk51WkTa0
[ix] Table D-2 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[x] Threats, vulnerabilities and exploits - https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my
[xi] Sheldon Adelson is winning his war against online gambling - http://www.forbes.com/sites/nathanvardi/2014/06/03/sheldon-adelson-is-winning-his-war-against-online-gambling/#9ef121292fef
[xii] Chronology of data breaches - https://www.privacyrights.org/data-breaches
[xiii] Fake PokerStars Skype phishing scam - https://www.pokerstrategy.com/news/content/Fake-PokerStars-Skype-Phishing-Scam_49023/
[xiv] Kerchoffs's Principle http://www.crypto-it.net/eng/theory/kerckhoffs.html
[xv] "How we learned to cheat at online poker" - http://www.datamation.com/entdev/article.php/11070_616221_2/How-We-Learned-to-Cheat-at-Online-Poker-A-Study-in-Software-Security.htm
[xvi]PokerStars security highlights - https://www.pokerstars.uk/poker/room/features/security/
[xvii] "PokerStars account hacks lead to questions about site's security" - http://www.flushdraw.net/news/pokerstars-account-hacks-lead-to-questions-about-sites-security/

# 4 Appendix

Table 2: Vulnerabilities and control measures

| Vulnerability | Potential exploits | Threat agents | Motive | Existing control measures |
|---|---|---|---|---|
| **Unauthorised system access** | Brute force password cracking<br><br>Forgotten password systems<br><br>Social engineering attacks<br><br>Forgotten password systems | Hackers, criminals | Theft of money from user accounts<br><br>To obtain customer information.<br><br>To gain an unfair advantage in games | Account passwords. Separate display names and email addresses. Email address is not shared publicly. Minimum password length of 8 characters. Restricted number of login attempts. |
| **Interception of data** | Eavesdropping<br><br>Software tampering | Hackers, criminals, users | Theft of money from user accounts<br><br>To obtain customer information | Encryption of data with AES128-SHA and DES-CBC3-SHA ciphers. RSA 2048 bit encryption certificate in software installer. Regular server key review. Client input validated server side. |
| **Failure of software** | Flaws in software design | Users | Users could exploit problems to gain an unfair game advantage | Methodology for random number generation is public. |
| **Denial of service** | Flaws in software design | Hackers, criminals | Vandalism, data theft | Restricted to one account per person. Must play poker games through proprietary software. |

Table 3: Threats-vulnerability pairs

| | VULNERABILITY | THREAT | IMPACT | LIKELIHOOD | RISK |
|---|---|---|---|---|---|
| 1 | Unauthorised system access | Unauthorised users obtaining customer information from databases | **High.** If data was breached in this way many customers would be affected. Their personal information could be widely circulated and potentially their financial data could be stolen. Confidentiality and availability controls would be breached. There would be little course of action available to mitigate the damage post loss.<br><br>There would be significant reputational repercussions for PokerStars and it would likely damage their standing in the industry, losing customers / money. | **Low.** There are strong countermeasures in place such as a dedicated secure data warehouse with biometric access control.<br><br>An attacker would need to have advanced capabilities and resources. | **Medium.** This type of attack succeeding is unlikely because of the strong security measures in places, however the consequences would be severe for PokerStars and its users if it were to happen. |
| 2 | Unauthorised system access | Unauthorised users obtaining account details through social engineering, phishing scams | **Low.** Data breaches of this sort usually only affect small numbers of users. Although an attack could have a big impact on individual customers, PokerStars itself would not be greatly harmed unless it became much more prevalent.<br><br>Phishing diminishes the integrity of PokerStars data to trick users into divulging information. | **High.** Social engineering and phishing attacks take place all the time.<br><br>These types of attacks are difficult to eradicate because of the low level of capability and resources required to launch them. | **Low.** These attacks are commonplace and generally accepted within the risk tolerance of online customers. |
| 3 | Interception of data | Unauthorised users obtaining customer information by eavesdropping methods | **Medium.** Potentially many customers could be affected by this type of attack however not as many as in a full database theft. The problem would likely be caught relatively quickly and the effects minimised.<br><br>There would likely be some reputational damage in the event of this sort of attack. | **Low.** There are strong countermeasures in place such as industry standard encryption of data.<br><br>An attacker would need to have advanced capabilities and resources. | **Low.** This type of attack is well defended against and its effects could be mitigated. A large attack could cause significant damage to PokerStars and its user base, however. |
| 4 | Failure of software | Players gaining unfair advantages by exploiting flaws in the shuffle algorithm | **Very high.** If this scenario developed, individual customers would be exploitable by cheaters.<br><br>For an online poker site, game integrity is one of the highest profile security issues. Should a failure take place the reputational damage would be catastrophic and it is possible that most players would leave the site. | **Low.** There are strong countermeasures in place such as the mathematically strong methodology in place for random number generation. | **Medium.** This type of system failure is much less likely to take place in the relatively mature online poker market than it was a decade or more ago, but if it did consequences would be catastrophic for PokerStars. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Denial of service | Malicious parties launching denial of service attacks | **Medium**. Denial of service outages result in lost business hours which mean a resultant lost revenue.<br><br>There is also a reputational risk and if the problem became severe enough customers could look to other platforms. | **High**. These attacks take place constantly. However, there are few enough service outages to suggest that systems are robust and there are strong countermeasures in place, such as only allowing one account per person. Denial of service attacks are very difficult to prevent entirely. | **Medium**. Denial of service attacks could present serious problems for PokerStars but the risk is managed well at this time. |

Figure 3: Password creation

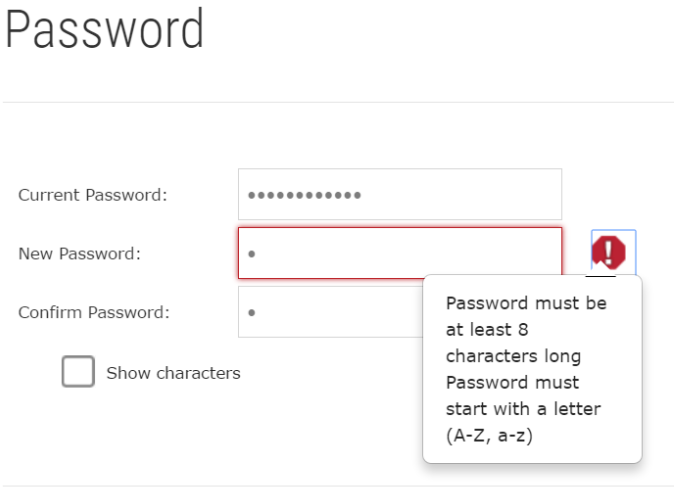


Figure 4: Password reset email (username redacted)