Um estudo sobre a segurança da informação em jogos online

Thiago Ferreira Dantas[1], Patricia Padula Lopes[1], Mariana Pompeo Freitas[1], Érico Marcelo Hoff do Amaral[1]

[1]Engenharia de Computação – Universidade Federal do Pampa (UNIPAMPA)
Avenida Maria Anunciação Gomes de Godoy, 1650 – 96.413-172 – Bagé – RS – Brasil

{padulalopes, thiagodantas923, maripompeof, ericohoffamaral}@gmail.com}

Abstract. *Considering the technological progress and their repercussion in social contacts, the present study investigated the relationship between the practice of online games on the Internet and its relationship with information security in a group of 112 people. Therefore, a questionnaire was elaborated and applied that addressed aspects such as the posture of the players regarding the availability of information, private and relevant, to other players in the network. The results indicated that the main vulnerabilities are in their own users who are not aware of the scams that happen in the network and do not take the necessary precautions.*

Resumo. *Considerando o progresso tecnológico e a repercussão dos mesmos nos contatos sociais, o presente estudo investigou a relação entre a prática de jogos online na internet e sua relação com a segurança da informação em um grupo de 112 pessoas. Para tanto, elaborou-se e aplicou-se um questionário que abordou aspectos como a postura dos jogadores em relação a disponibilização de informações, privadas e relevantes, para outros jogadores na rede. Os resultados indicaram que as principais vulnerabilidades estão em seus próprios usuários que não estão cientes dos golpes que acontecem na rede e não tomam as devidas precauções.*

1. Introdução

Esta pesquisa apresenta um diferencial das já existentes visto que pouco enfoque tem sido dado ao estudo sobre a segurança em *games*, sejam eles de computador, vídeo *game* ou celular. Visando suprir esta deficiência, este trabalho se propõe a questionar sobre as principais vulnerabilidades que podem ser exploradas por cibercrimosos e até mesmo por outros jogadores em jogos *online* na *internet*, visto que cerca de 74,4% dos brasileiros jogam em algum dispositivo eletrônico e encontram-se vulneráveis por estarem conectados à internet (SIOUX, 2016). Com números expressivos, o setor também se apresenta como um potencial alvo para os criminosos virtuais.

A facilidade de comunicação entre os jogadores, somado ao alto grau de confiança que os usuários costumam depositar entre si, fez com que os jogos online ganhassem grande popularidade e chamassem a atenção, também, de pessoas mal-intencionadas. Além de poder enviar *links* e arquivos maliciosos por intermédio de *chats* ou de mensagens online dentro do jogo, cibercriminosos podem usar os jogos para

cometer *cyberbullying*, atrair crianças, adolescentes e até mesmo adultos para atos ilícitos. Existem também, alguns jogos que oferecem créditos, ferramentas e benefícios que podem ser comprados ou conquistados pelos jogadores. Além do risco de ter dados do cartão de crédito hackeados, jogadores mal intencionados podem usar essas ferramentas como forma de chantagens.

Devido à alta interatividade e conectividade de seus usuários, este tipo de aplicação vem ganhando novos usuários a cada dia, e consequentemente, os problemas citados acima passam a ser cada vez mais comuns. Por este motivo, pretende-se problematizar, a partir de um estudo exploratório, os riscos envolvidos na segurança da informação associados a jogos online na internet.

Para apresentar este estudo, o presente artigo foi estruturado em 4 seções. Na Seção 2 é realizado o levantamento teórico sobre conceitos relevantes para o desenvolvimento do trabalho. A Seção 3 apresenta a caracterização da pesquisa e os procedimentos metodológicos adotados. A Seção 4 contém os resultados atingidos. E por fim, na Seção 5 são apresentadas as considerações parciais.

2. Referencial Teórico

2.2 A Segurança em jogos online na internet

Por estarem conectados ao mundo inteiro, jogadores podem interagir com outras pessoas de várias formas. Com esse nível de interação surgem riscos, especialmente os vírus, o roubo de identidade virtual e os ataques *phishing* onde o atacante cria, por exemplo, uma réplica de uma página, que pode ser de um jogo na web, para enganar os usuários, fazendo com que eles enviem dados ou senhas, pensando que é um site de seus prestadores de serviços (SILVEIRA *et.al* 2017).

Ao interagir socialmente com estranhos, que podem enganar e até mesmo fazer com que informações pessoais ou financeiras, sejam reveladas, há também os riscos envolvidos na invasão do computador do usuário se aproveitando de vulnerabilidades do sistema operacional. Boa parte dos golpes relacionados a *games* são direcionados para quem joga no computador e, entre todas as fraudes, a possibilidade de instalar um software indesejado é provavelmente a mais séria.

Há também alguns *softwares* indesejados que são utilizados por outros jogadores, dentro do jogo, que realizam trapaças ou que permitem jogar sem uma licença do *software*, ou seja, "*patches*", "*trainers*", "*bots*" e "pirataria". É preciso muito cuidado ao buscar *trainers* e *patches*: esses podem criar novas funcionalidades e aumentar a diversão do *game*. Porém, é importante salientar que a pirataria é considerada um ato ilícito, considerado crime pelo artigo 184 do Código Penal Brasileiro. E que assim como os *bots*, que são *softwares* de trapaça, eles também são proibidos, porque oferecem vantagens irregulares a quem os instala.

Há ainda, os riscos envolvidos na compra de itens virtuais que melhoram o desempenho e permitem ultrapassar os níveis mais difíceis do jogo. Para obter estes itens, é possível negociar entre os jogadores ou comprá-los através do game, por meio de cartão de crédito, dinheiro ou moeda virtual. Ainda existe a possibilidade de adquirir estes itens através de mercados não oficiais, proibidas pelos desenvolvedores e muitas vezes mantidos por golpistas, que roubam desde itens utilizados nos jogos até senhas

usando *softwares* indesejáveis. Participar desse tipo de mercado é um risco, pois não há garantia de que se irá receber as "mercadorias virtuais".

Diante do exposto, é possível perceber que há perigos bem reais do uso inconsciente destes tipos de aplicativos: riscos de ser furtado, excesso de exposição, e complicações na vida pessoal por divulgação de informações privadas. Por isso, pretende-se demonstrar ao leitor os riscos envolvidos com algumas práticas em jogos online e alertar quanto as ações que podem ser tomadas, permitindo intervenções preventivas para evitar que pessoas mal intencionados consigam ludibriar suas vítimas.

3. Metodologia

De acordo com os métodos descritos na literatura, a pesquisa constitui-se como quantitativa visto que traduz em números as opiniões e informações sobre vários aspectos que abordam a segurança de jogos online na internet para serem classificados e analisados, utilizando-se para isto técnicas estatísticas (GÜNTHER, 2009).

Tendo em vista a metodologia adotada para o desenvolvimento deste trabalho, na Figura 1 é apresentado um resumo de cada uma das etapas para o desenvolvimento deste estudo.

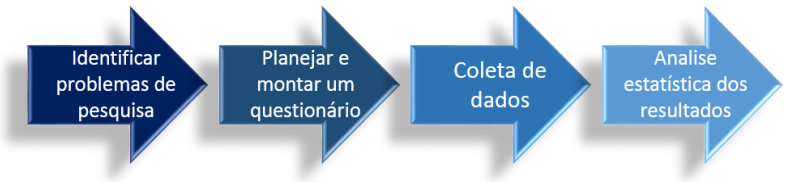

Figura 1. Etapas da Metodologia

Inicialmente, identificou-se a necessidade de um estudo relacionado a segurança da informação em jogos, visto que há uma defasagem em trabalhos referentes a este tema. O instrumento de pesquisa escolhido para este estudo foi um questionário, composto de 30 questões sobre aspectos relacionados a segurança da informação num contexto do jogo eletrônico online. Os itens do questionário pretenderam investigar hábitos dos participantes ao jogar e verificar se estes podem fazer com que os jogadores passem a ser vítimas de pessoas mal intencionadas (falsificadores, golpistas, pedófilos, entre outros).

Para a coleta dos dados, o questionário foi disponibilizado na internet nas principais páginas *gamers* para quem tem Facebook, dentre elas: Mayday, grupo GamesIndie, Ilha da Macacada, e também em grupos fechados da Universidade Federal do Pampa. Destes, foram respondidos 112 questionários, os quais representam o presente estudo. Com isto, foram apurados os dados relevantes para esta pesquisa.

4. Resultados e Discussões

Considerando os resultados obtidos com a aplicação dos questionários, foi possível verificar que a grande maioria dos entrevistados costuma jogar frequentemente, por pelo menos uma ou mais horas por dia, porém não sabem se proteger das ameaças que os cercam diariamente, devido à falta de informação dos riscos que possuem durante a navegação e exposição de suas informações.

Do total de membros pesquisados, 66,1% revelaram dados pessoais como seu nome completo em mensagens via *chat* com outros jogadores, dentre estes, 58,3% passam contatos do seu perfil do Facebook para outros jogadores na rede. Dentre estes, apenas 29,6% não passam nenhum contato de suas redes sociais ou endereço pessoal (Figura 5). Cabe salientar que o Facebook é aberto para qualquer pessoa que tiver interesse em se cadastrar, basta acessar o site e preencher as informações solicitadas para criação de perfil. Dentre essas informações estão locais que os usuários frequentam, onde residem, seus horários, números de celulares entre outras informações que podemos considerar de uso pessoal ou familiar, que podem ser disponibilizadas pelos usuários a suas conexões. Entende-se que um perfil em um site de rede social fornece a pessoas mal intencionadas subsídios suficientes para ataques de engenharia social (TEIXEIRA *et al.* 2013).

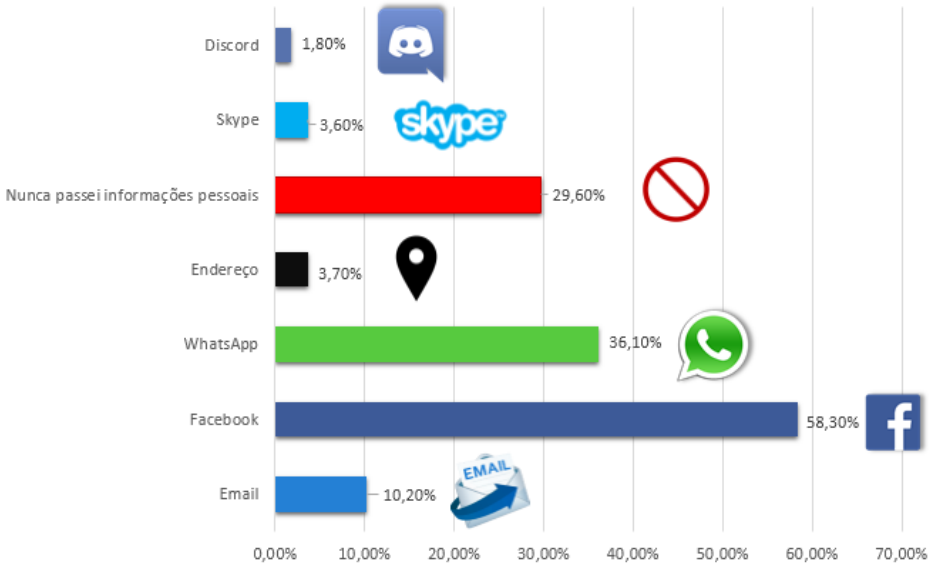

Figura 2. Passam contatos pessoais para outros jogadores

Outro ponto relevante na pesquisa foi com relação aos jogadores que já sofreram algum tipo de trapaça, como pode ser visto no gráfico da Figura 6, 46% foram engados por outros usuários que contornam as regras do jogo ou exploram ainda erros que encontram no código do jogo para ter mais vantagens. No entanto, dentre os entrevistados, 44% já relataram que utilizaram algum programa ilegal para facilitar o jogo.

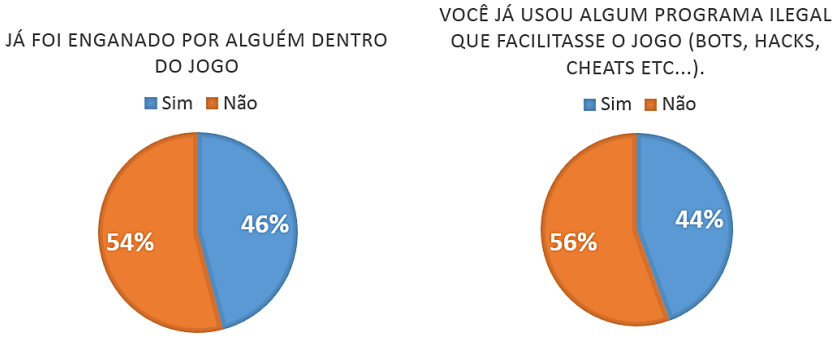

Figura 3. Já foi enganado ou foi enganado

Além disso, 48,2% afirmaram que receberam propostas suspeitas quanto aos itens que são vendidos nos games, como por exemplo, itens sendo vendidos muito abaixo do preço normal, onde a maioria dos jogadores aceitou as ofertas e os itens valiosos de desconhecidos nos jogos, até mesmo, em troca de informações pessoais. De acordo com as respostas, 77,7% aceitariam baixar programas e informar senhas dos jogos para obtenção de vantagens ou ter acesso ao jogo. Com base no gráfico da Figura 7, 32,4% alegaram terem tido uma conta *hackeada* ou roubada em algum jogo *online*.

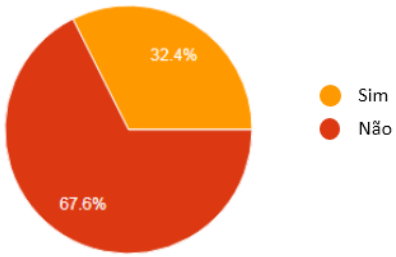

Figura 4. Teve alguma conta em algum jogo hackeada ou roubada

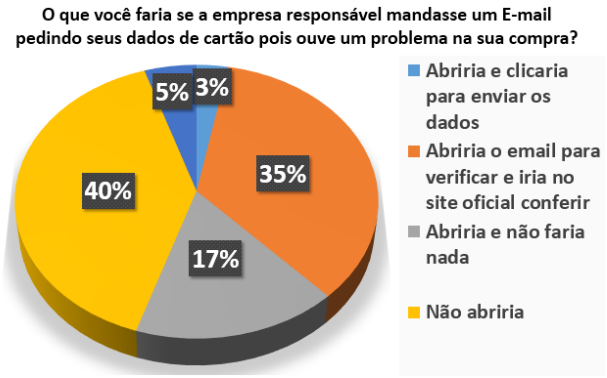

Figura 5. Envio de dados de cartão de créditos por e-mail

Um dos possíveis fatores responsáveis por isso pode ser a não utilização de senhas fortes e únicas, onde 30,4% relataram adotar práticas de senhas inseguras quando criam suas contas.

Dentre estas pessoas 81,1% já investiu dinheiro real em algum jogo *online* ou comprou algum jogo de lojas como a Steam ou Origin. Quando questionados sobre o envio dos dados de seu cartão de crédito para a empresa responsável pelo jogo, 35% disseram abrir o *e-mail* e conferir se havia alguma informação no site oficial da organização, 17% abririam e não fariam nada e 3% enviariam seus dados (Figura 8).

A partir das respostas auferidas pelos entrevistados pode-se concluir que os jogadores podem estar sujeitos a várias ameaças que comprometem seriamente a sua segurança, é aconselhável de acordo com as medidas de proteção apontadas pela Intel Security que os usuários, nunca façam *downloads* de jogos e aplicativos fora das lojas oficiais e não comprem jogos piratas. Cibercriminos podem criar sites e aplicativos falsos com intuito de espalhar *malwares* e roubar dados. Criminosos também podem enviar mensagens e *e-mails* falsos relacionados aos jogos solicitando troca de senha ou alteração de cadastro essa técnica é usada para roubar dados dos usuários. Outra medida de segurança, é evitar salvar dados bancários e de cartões de créditos em jogos online e aplicativos, pois estes dados podem ser clonados por algum *cracker*. No caso dos *games* em que os jogadores podem trocar arquivos e mensagens, é recomendado que não se forneça informações pessoais para desconhecidos em *chats* de jogos, como contatos de redes sociais.

5. Considerações Finais

Com base nos resultados, pode-se perceber que vários jogadores estão vulneráveis a pessoas mal-intencionadas, ao disponibilizaram informações pessoais. Muitos já foram engados durantes as partidas, mas também já tentaram se beneficiar de outros jogadores. Outros, não tomam cuidado para proteger-se no ambiente virtual e podem ser alvos fáceis de atacantes que utilizam técnicas de *phishing* e enganam os usuários para obtenção de dados privados e senhas. Haja vista que, como já mencionado por Silveira *et.al* (2017), a maior vulnerabilidade é o próprio usuário e sua atitude para com a segurança digital que na maioria das vezes não estão preparados para lidar e reconhecer situações de riscos.

Referências

ABRAGAMES. **A indústria brasileira de jogos eletrônicos: um mapeamento do crescimento do setor nos últimos 4 anos.** Pesquisa 2008, versão 1.0. Brasil, julho de 2008. Disponível em: <www.abragames.org>. Acesso em: 20 de novembro de 2017.

INTEL SECURITY. ***Internet security measures*** <http://www.intelsecurity.com/>. Acesso em: 09 de novembro de 2017.

NPD GROUP. ***More Americans Play Video Games Than Go Out to the Movies.*** Estados Unidos. Disponível em: <http://www.npd.com/press/releases/press_090520.html>. Acesso em: 10 de novembro de 2017.

GÜNTHER, Hartmut. **Pesquisa Qualitativa versus Pesquisa Quantitativa: Esta é a questão?** Disponível em <http://www.scielo.br/pdf/ptp/v22n2/a10v22n2.pdf>. Acesso em set. 2017.

PYLRO, Simone Chabudee; ROSSETTI, Claudia Broetto; GARCIA, Agnaldo. **Relações de amizade e prática de jogos online: um estudo exploratório com adolescentes.** Interação em Psicologia, v. 15, n. 1, 2011.

SILVEIRA, Lucidia et al. **Segurança em Redes Sociais Online: Reconhecendo Ameaças.** Anais SULCOMP, v. 8, 2017.

SIOUX. **Pesquisa games brasil 2016.** Disponível em:<http://media.wix.com/ugd/29fc6b_a41f6959f6314fb8bfe60bb18ae462c8.pdf>. Acesso em 16 nov. 2016.

TEIXEIRA, Elenir Custódio; AGUADO, Alexandre Garcia. **Segurança da Informação nas Redes Sociais**. Revista Network Technologies Faculdades Network–Revista da Faculdade de Sistema de Informação ISSN 1677-7778, p. 77, 2013.

TRINCA, Daniel et al. **Jogos online**. Revista de Informática Aplicada, v. 2, n. 1, 2010.