**FICHAMENTO DO ARTIGO – Vale 2,0 PT.**

**ENTREGA 25/04**

**SIA**

**Artigo: “O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing”**

**Disponível em: https://sol.sbc.org.br/index.php/sbsi/article/view/5694/5591)**

Aluno(a): Cauã Thurler Pinheiro de Azevedo

Responda: O aluno deverá entregar um resumo do artigo de no mínimo duas páginas, onde a conclusão deverá ter a impressão pessoal do aluno a respeito do tema abordado.

Em face ao atual cenário global interconectado, o meio virtual se tornou uma extensão do cotidiano dos indivíduos, sendo, não só um meio de comunicação e informação, mas também um meio de entretenimento, expansão das relações pessoais, trabalho, entre outros. Com isso, critérios aplicados em outras áreas da vida começaram a ser aplicados no contexto digital e, entre outros muitos temas, muito se tem estudado sobre a questão da segurança.

Tendo em vista a necessidade do aprofundamento do debate sobre a segurança da informação, podemos identificar a relevância do tema em questão. De acordo com o artigo "O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing" dos autores Gliner Dias Alencar, Marcelo Ferreira de Lima e André C. A. Firmo e publicado pelos anais do IX Simpósio Brasileiro de Sistemas de Informação ocorrido no ano de 2013, são necessárias ações gerenciais de tratamento e melhora dos processos, tecnologias e pessoas para quer o tratamento da segurança da informação nos dias atuais seja efetivo.

O estudo aplicou um treinamento de engenharia social e phishing para 30 funcionários de diferentes setores em uma empresa, durante 2 dias, com 2 horas de treinamento por dia. Metade dos funcionários treinados recebeu boletins de segurança durante 4 semanas, alertando sobre ameaças de engenharia social e phishing. Depois de 15 dias, foi enviado um e-mail por dia com phishing para a conta de e-mail corporativo de 45 usuários, incluindo 15 do grupo que recebeu o treinamento e o reforço por e-mail, 15 que receberam apenas o treinamento e 15 que não participaram do treinamento. Todos os e-mails consistiam em imitações de bancos ou serviços de e-mail populares, e um clique no link do e-mail contabilizava um clique, sem mais cliques contados para o mesmo e-mail.

A pesquisa foi realizada em quatro empresas privadas do Recife que não atuavam na área de TI. Foram criados três grupos de 15 funcionários em cada empresa para avaliar o nível de informação e conscientização sobre segurança da informação. Foram aplicados treinamentos de engenharia social e phishing para metade dos funcionários, seguido de boletins de segurança e phishing. O teste consistiu em enviar e-mails com phishing para os funcionários durante 21 dias, sendo avaliado o número de cliques nos links maliciosos. A pesquisa também avaliou a existência e divulgação de Políticas de Segurança da Informação (PSI) nas empresas.

A pesquisa analisou quatro empresas privadas sem atividades relacionadas a TI em Recife. Foram criados três grupos em cada empresa para avaliar o nível de informação e conscientização sobre segurança da informação (SI). Os resultados indicaram que os grupos com capacitação e reforço em engenharia social e phishing apresentaram menos cliques em armadilhas, em comparação com o grupo sem treinamento. A empresa C teve os piores resultados, enquanto a empresa B teve os melhores, apesar de ambas estarem no mesmo estágio de maturidade em SI. A empresa D, com a menor maturidade, obteve a terceira colocação, e a empresa A, com teoricamente maior maturidade, obteve a segunda colocação. Os resultados indicam a importância da capacitação e do reforço periódico, independentemente do nível de maturidade da empresa, para a melhoria na detecção de phishing.

Uma pesquisa demonstrou que a engenharia social e o phishing continuam sendo um meio eficaz de obtenção de dados de funcionários em ambientes corporativos, especialmente quando se trata de dados internos da empresa. O estudo destaca a importância da capacitação e conscientização contínua dos funcionários como um fator de elevação do grau de segurança da informação na corporação, fortalecendo o elo mais fraco da segurança da informação em uma corporação. O autor enfatiza que a segurança da informação deve ser entendida como responsabilidade de todos e que uma mudança no pensamento de todos os envolvidos é necessária. O estudo conclui que uma política completa de divulgação, treinamento e conscientização é necessária para incorporar as práticas de segurança na rotina de trabalho de todos os funcionários, desde o pessoal operacional até os executivos de alto nível. O autor destaca a importância da educação em vez de apenas treinamento, pois o treinamento isolado é ineficaz diante das mudanças contínuas na tecnologia e nos métodos usados pelos atacantes.

Pra mim essa pesquisa destaca a importância da conscientização e capacitação dos funcionários para o combate à engenharia social e phishing em ambientes corporativos. É fundamental que empresas implementem políticas de segurança da informação abrangentes que incluam treinamentos contínuos, boletins de segurança e testes de phishing para garantir que seus funcionários estejam cientes dos riscos e saibam como identificar e evitar ataques.