

Como se Proteger de Golpes na Internet:
Uma Abordagem Educativa para a Comunidade de Nova Mutum

Alessandre dos Santos Julio; Fábio Honório da Silva; Gabriel Campos Cajaiba; Jacson Aparecido Franquelino Porto; Marcelo Bomdespacho da Conceição; Waldecy Rebouças Rabelo; João Ricardo Miranda de Andrade; Izabella Caroline Rocha Ribeiro; Fábio Vinicius das Neves Tosatti; Saymon Lopes Georg; Gleyniston Weyne da Silva de Sousa; Wendell Marques.

Orientadora: Pollianna Mesquita de Moraes

Nova Mutum-MT

06/2026

RESUMO

O crescimento do uso da internet e dos meios digitais de pagamento trouxe inúmeros benefícios para a sociedade, mas também ampliou a incidência de golpes virtuais que afetam milhões de brasileiros. Entre os grupos mais vulneráveis estão os idosos, que frequentemente apresentam dificuldades para identificar fraudes eletrônicas e mecanismos de engenharia social utilizados por criminosos. O presente artigo tem como objetivo relatar uma ação extensionista de conscientização sobre segurança digital realizada com idosos na cidade de Nova Mutum-MT. A metodologia adotada consistiu em pesquisa bibliográfica sobre crimes cibernéticos e elaboração de material educativo, seguida da realização de uma palestra em uma igreja da comunidade local. Durante a intervenção foram apresentados os principais tipos de golpes praticados na internet, incluindo phishing, clonagem de WhatsApp, golpe do Pix, lojas virtuais falsas e fraudes envolvendo inteligência artificial e deepfakes. A ação buscou fornecer orientações práticas de prevenção e esclarecimentos sobre os procedimentos adequados em caso de fraude. Os resultados observados indicaram interesse e participação ativa do público, demonstrando a relevância de iniciativas educativas voltadas à inclusão e proteção digital da população idosa. Conclui-se que ações de conscientização representam importante instrumento de prevenção, contribuindo para a redução da vulnerabilidade digital e para o fortalecimento da cidadania no ambiente virtual.

Palavras-chave: Segurança Digital; Crimes Cibernéticos; Idosos.

ABSTRACT

The growth of internet usage and digital payment systems has brought several benefits to society, but it has also increased the incidence of cyber fraud affecting millions of people. Among the most vulnerable groups are elderly individuals, who often face difficulties in identifying online scams and social engineering techniques used by criminals. This article aims to report an extension project focused on digital security awareness carried out with elderly people in the city of Nova Mutum-MT. The methodology consisted of a bibliographic review on cybercrime and the development of educational materials, followed by an awareness lecture held at a local church. During the intervention, participants were introduced to the main types of internet scams, including phishing, WhatsApp account cloning, Pix fraud, fake online stores, and scams involving artificial intelligence and deepfakes. The activity sought to provide practical prevention guidance and information on the appropriate measures to be taken in case of fraud. The results indicated active participation and interest from the audience, highlighting the relevance of educational initiatives aimed at promoting digital inclusion and protection among elderly citizens. It is concluded that awareness actions are important preventive tools that contribute to reducing digital vulnerability and strengthening digital citizenship.

Keywords: Digital Security; Cybercrime; Elderly People.

1. INTRODUÇÃO

A transformação digital modificou profundamente a forma como as pessoas se comunicam, realizam compras, acessam serviços públicos e efetuam transações financeiras. Paralelamente aos benefícios proporcionados pela tecnologia, observa-se o aumento significativo dos crimes praticados no ambiente virtual. Golpes realizados por meio de mensagens falsas, redes sociais, aplicativos de mensagens e sistemas de pagamento instantâneo tornaram-se cada vez mais frequentes, exigindo da população maior conhecimento sobre segurança digital.

Os idosos figuram entre os grupos mais suscetíveis a esse tipo de fraude devido às dificuldades de adaptação às novas tecnologias e à falta de acesso a informações especializadas sobre proteção digital. Nesse contexto, a educação preventiva surge como importante mecanismo de proteção social, permitindo que os cidadãos reconheçam situações de risco e adotem medidas de segurança adequadas.

Diante dessa realidade, o presente trabalho teve como objetivo promover uma ação de conscientização voltada à população idosa do município de Nova Mutum-MT, apresentando orientações práticas para identificação e prevenção dos principais golpes aplicados na internet.

Para alcançar esse objetivo, foi realizada pesquisa bibliográfica sobre segurança digital, crimes cibernéticos e legislação aplicável, seguida da elaboração de material educativo e da realização de palestra informativa junto à comunidade.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Segurança Digital e Crimes Cibernéticos

A expansão das tecnologias digitais transformou significativamente a forma como as pessoas realizam atividades cotidianas, como comunicação, compras, operações bancárias e acesso a serviços públicos. Entretanto, o avanço tecnológico também favoreceu o crescimento dos crimes praticados no ambiente virtual, exigindo maior atenção quanto à proteção de dados e à segurança das informações.

Segundo Peck (2021), a segurança digital não se limita à utilização de ferramentas tecnológicas de proteção, mas envolve também a conscientização dos usuários quanto aos riscos existentes no ambiente virtual. Para a autora, a educação digital constitui uma das principais estratégias de prevenção contra fraudes eletrônicas e violações de dados pessoais.

Os crimes cibernéticos caracterizam-se pela utilização de recursos tecnológicos para obtenção de vantagem ilícita, acesso indevido a sistemas, fraude eletrônica ou obtenção de dados pessoais sem autorização. Tais práticas apresentam constante evolução, acompanhando o desenvolvimento das tecnologias de comunicação e dos meios digitais.

2.2 Principais Golpes Aplicados na Internet

Entre os golpes mais frequentes estão o phishing, a clonagem de contas em aplicativos de mensagens, fraudes envolvendo transferências via Pix, lojas virtuais falsas e, mais recentemente, golpes praticados com o auxílio da inteligência artificial.

O phishing consiste na utilização de mensagens fraudulentas que simulam comunicações legítimas de instituições financeiras, empresas ou órgãos públicos com o objetivo de induzir a vítima ao fornecimento de informações pessoais e bancárias. Já a clonagem de contas em aplicativos de mensagens ocorre quando criminosos assumem a identidade digital da vítima para solicitar transferências financeiras a familiares e amigos.

Outro golpe recorrente envolve a criação de lojas virtuais falsas, nas quais produtos são anunciados a preços atrativos sem que haja a efetiva entrega ao consumidor. Nos últimos anos, também se destacaram as fraudes realizadas por meio de deepfakes, tecnologia capaz de reproduzir voz e imagem de terceiros para enganar vítimas e obter vantagens financeiras.

2.3 Embasamento Legal da Proteção Digital

O ordenamento jurídico brasileiro possui importantes instrumentos destinados à proteção dos usuários da internet e ao combate aos crimes cibernéticos.

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Entre seus princípios fundamentais destacam-se a proteção da privacidade, a proteção dos dados pessoais e a preservação da segurança da rede. O artigo 3º determina que a disciplina do uso da internet deve observar a proteção da privacidade e dos dados pessoais dos usuários.

Complementando esse sistema de proteção, a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais em meios físicos e digitais. O artigo 1º estabelece que a finalidade da lei é proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural. O artigo 2º apresenta como fundamentos da proteção de dados o respeito à privacidade, a autodeterminação informativa e a defesa dos direitos fundamentais dos cidadãos.

No âmbito penal, destaca-se a Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, que introduziu no Código Penal o crime de invasão de dispositivo informático. O artigo 154-A prevê punição para quem invadir dispositivo eletrônico mediante violação indevida de mecanismo de segurança com o objetivo de obter, adulterar ou destruir dados sem autorização do titular.

Conforme Doneda (2021), a proteção de dados pessoais deve ser compreendida como um direito fundamental relacionado à dignidade da pessoa humana, exigindo do Estado e da sociedade mecanismos eficazes de prevenção e responsabilização diante das violações ocorridas no ambiente digital.

2.4 Educação Digital como Ferramenta de Prevenção

A conscientização da população constitui uma das principais estratégias para redução dos crimes cibernéticos. A adoção de práticas seguras de navegação, utilização de senhas fortes, autenticação em dois fatores e verificação da autenticidade de mensagens recebidas contribui significativamente para a diminuição das vulnerabilidades digitais.

Nesse contexto, as ações extensionistas desenvolvidas pelas instituições de ensino superior assumem papel relevante ao aproximar o conhecimento acadêmico das necessidades da comunidade. Por meio de palestras, campanhas educativas e atividades de orientação, torna-se possível promover a inclusão digital e fortalecer a proteção dos cidadãos contra fraudes eletrônicas.

3. METODOLOGIA

A pesquisa caracteriza-se como bibliográfica, descritiva e de natureza qualitativa. Inicialmente foi realizado levantamento de informações em artigos científicos, legislações, relatórios institucionais e publicações relacionadas à segurança digital e aos crimes cibernéticos.

O público-alvo da ação extensionista foi composto por aproximadamente vinte idosos participantes de uma igreja localizada no município de Nova Mutum-MT. A escolha desse público ocorreu em razão da vulnerabilidade frequentemente observada dessa faixa etária diante de golpes praticados por meios digitais.

Com base no levantamento teórico, foi elaborado material educativo contendo informações sobre os principais golpes na internet, suas características e formas de prevenção. Posteriormente, foi realizada uma palestra presencial de caráter informativo e preventivo, na qual foram apresentados exemplos práticos de phishing, clonagem de WhatsApp, golpes envolvendo Pix, lojas virtuais falsas e fraudes realizadas com o uso de inteligência artificial.

A intervenção teve como finalidade ampliar o conhecimento dos participantes sobre segurança digital, incentivando práticas seguras de navegação, proteção de dados pessoais e adoção de medidas preventivas contra fraudes virtuais.

4. RELATO DA INTERVENÇÃO EXTENSIONISTA

A ação extensionista foi realizada em uma igreja do município de Nova Mutum-MT, reunindo aproximadamente vinte participantes idosos. Durante a atividade foi apresentada uma palestra educativa com linguagem acessível e exemplos práticos do cotidiano.

Inicialmente foram discutidos os riscos existentes no ambiente digital e os principais métodos utilizados por criminosos para obter informações pessoais e financeiras das vítimas. Em seguida, foram abordados os golpes mais frequentes registrados no Brasil, incluindo mensagens fraudulentas, clonagem de contas em aplicativos de mensagens, falsas ofertas comerciais, golpes relacionados ao Pix e fraudes envolvendo inteligência artificial.

Ao longo da apresentação foram fornecidas orientações práticas para identificação de sinais de fraude, criação de senhas seguras, utilização da autenticação em dois fatores e procedimentos recomendados em caso de golpe consumado. A participação dos presentes ocorreu por meio de perguntas, relatos de experiências e esclarecimento de dúvidas relacionadas ao uso da internet.

5. RESULTADOS E DISCUSSÃO

A intervenção possibilitou a disseminação de informações relevantes sobre segurança digital para um público considerado vulnerável aos crimes cibernéticos. Observou-se interesse dos participantes durante toda a atividade, especialmente nos temas relacionados aos golpes do Pix, clonagem de WhatsApp e mensagens fraudulentas.

A interação entre palestrantes e participantes demonstrou que muitos dos presentes já haviam recebido tentativas de golpes ou conheciam pessoas que haviam sido vítimas de fraudes digitais. Esse aspecto reforça a necessidade de ações educativas permanentes voltadas à conscientização da população.

Embora não tenha sido realizada pesquisa quantitativa para mensuração dos resultados, a receptividade do público e o envolvimento observado durante a palestra indicam que a ação contribuiu para ampliar o conhecimento dos participantes sobre práticas de proteção digital, fortalecendo a prevenção contra crimes cibernéticos.

6. CONSIDERAÇÕES FINAIS

Os golpes praticados na internet representam um dos principais desafios da sociedade contemporânea, exigindo medidas educativas capazes de fortalecer a segurança digital da população. Nesse contexto, a ação extensionista realizada demonstrou que atividades de conscientização constituem instrumentos eficazes para disseminação de informações e prevenção de fraudes.

A palestra desenvolvida junto aos idosos de Nova Mutum-MT permitiu abordar de forma acessível temas relacionados à proteção de dados, identificação de golpes e utilização segura dos recursos tecnológicos. Além de beneficiar a comunidade atendida, a atividade contribuiu para a formação acadêmica e cidadã dos estudantes envolvidos.

Conclui-se que iniciativas extensionistas voltadas à educação digital possuem grande relevância social, especialmente quando direcionadas a grupos mais vulneráveis, contribuindo para a construção de uma cultura de segurança e responsabilidade no ambiente virtual.

REFERENCIAS

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF, 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

PECK, Patrícia. Direito Digital. 8. ed. São Paulo: Saraiva Educação, 2021.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: comentários à Lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2020.

MARTINS, Guilherme Magalhães. Responsabilidade Civil por Acidentes de Consumo na Internet. São Paulo: Revista dos Tribunais, 2014.