# Contexto

Vivemos em uma era digital onde os dados são tão valiosos quanto o ouro. Ataques cibernéticos ocorrem frequentemente todos os dias, afetando desde usuários comuns até grandes corporações e governos.

Com isso, a segurança digital deixou de ser um tema técnico restrito a profissionais da área e passou a ser uma necessidade básica da vida moderna.

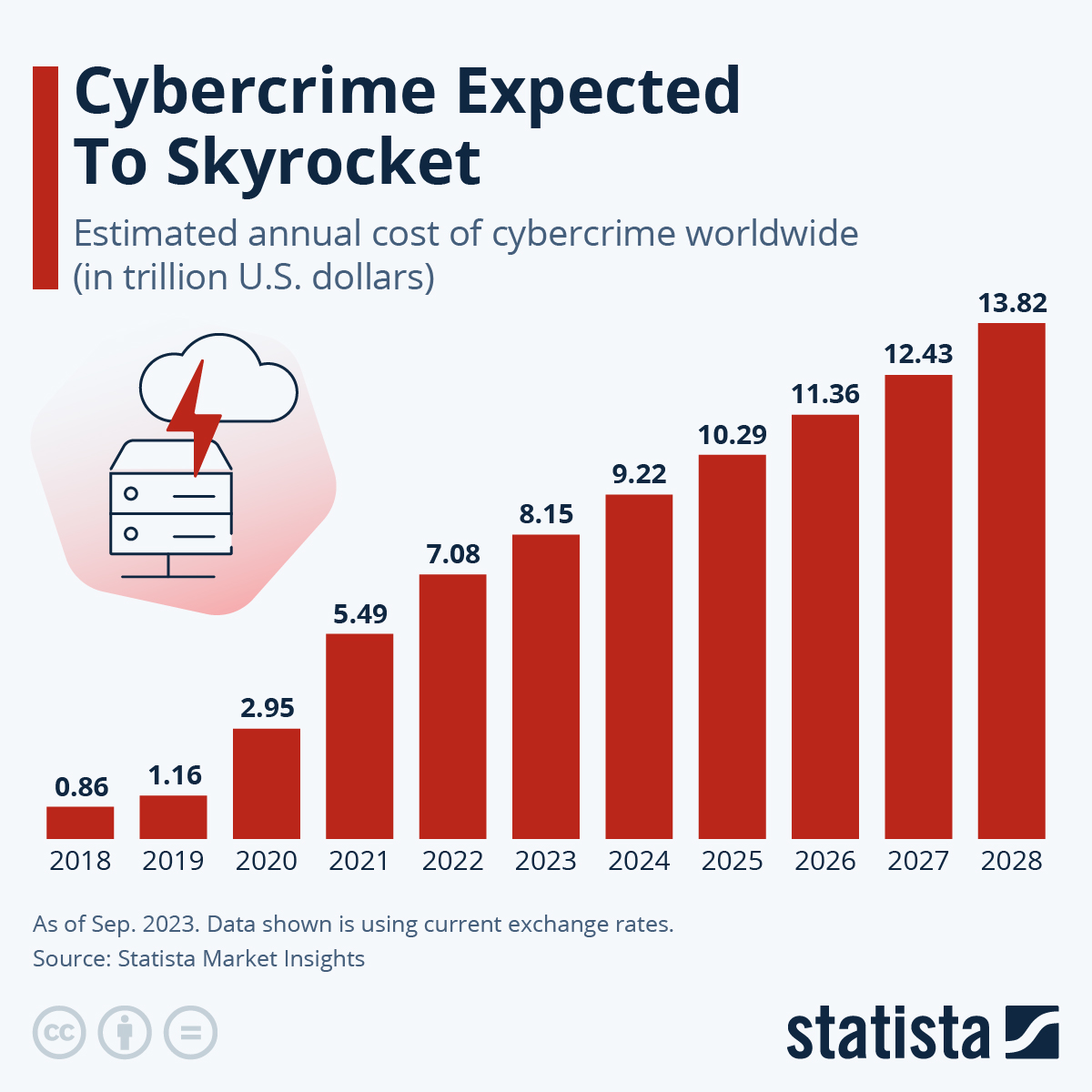


Além disso, o termo “Hacker” frequentemente é associado de forma equivocada a criminosos, quando na realidade existem diversos tipos de Hackers muitos dos quais atuam para proteger sistemas e garantir a integridade digital de empresas e pessoas.

Negligência em medidas de proteção contra ameaças online, como ataques cibernéticos, roubos de dados e fraudes pode ter consequências graves, incluindo perdas financeiras, danos à reputação e até mesmo perigo para a segurança pessoal.

Este projeto surge como uma forma de educar, informar e engajar, apresentando conceitos técnicos com uma linguagem acessível e conteúdos visuais envolventes.

Segundo um relatório da Cybersecurity Ventures, os danos financeiros causados pelo cibercrime podem atingir US$ 10,5 trilhões por ano em 2025, superando até mesmo o tráfico de drogas como uma das atividades ilícitas mais lucrativas.



# Objetivo

Objetivo Geral:

Promover a conscientização sobre segurança digital, desmistificar o Hacking e apresentar medidas práticas de proteção no ambiente online, com dicas e roteiros de ensinos básicos ao usuário.

Objetivos Específicos:

- Explicar o que é Hacking e seus diferentes tipos (White Hat, Black Hat, etc.).

- Ensinar boas práticas de segurança digital (uso de senhas fortes, autenticação em dois fatores, backups, etc.).

- Conscientizar sobre ameaças cibernéticas reais.

- Estimular o interesse no Hacking ético como carreira e desmitificar a área.

- Oferecer uma experiência interativa por meio de quizzes, vídeos e seções didáticas.

# Justificativa

A ideia do projeto parte de uma motivação pessoal e de uma realidade crítica: muitas pessoas estão vulneráveis por desconhecimento. A segurança digital ainda é vista de forma limitada, e é necessário mostrar que ela vai além do uso de antivírus. A iniciativa reflete a paixão do autor por tecnologia, inspirada desde a infância, e o desejo de transformar conhecimento em defesa. É um chamado para educar, proteger e inspirar uma nova geração digitalmente consciente.

# Valores e Motivação Pessoal

Este projeto reflete minha paixão pessoal pela área da tecnologia, segurança da informação e Hacking. Desde cedo, sempre fui curioso sobre como os sistemas funcionam, juntamente quando pequena via muitos filmes de ação sempre envolvia um pouco Hacking, filmes de super herói, as vezes haviam o nerd especialista em tecnologia, que conseguia invadir câmeras etc. Me chamando muito atenção, e trazendo este interesse, por isto iniciei minha jornada na tecnologia, porém em hardware.

Meu Objetivo desde pequeno era ter uma assistência técnica de computadores, voltado a manutenção avançada de placas eletrônicas. Nunca tive coragem de seguir área de programação, pois já achava muita dor de cabeça trabalhar com hardware, eu já imaginava que programação seria pior, no entanto por mais que eu tivesse vontade, por receios não progredi no assunto.

Como dito sempre fui apaixonado por filmes de ação, bem como o principal filmes e series contendo atiradores de elite, fiz curso técnico para seguir a área, e também mantive estudos na tecnologia por Hobbie, no entanto no meio desta formação desisti de seguir carreira militar por motivos pessoais.

Mesmo tendo essa paixão por tecnologia e muitos a minha volta me aconselhando seguir esta área, não me sentia seguro, não tinha visão dessa oportunidade. Porém, assim que tive a oportunidade de fazer parte do projeto da SPTECH, percebi que este sonho de criança deixou de ser sonho para ser uma meta de vida, sendo ela me formar em segurança digital.

Escolhi esse tema porque acredito que o conhecimento é a melhor defesa. Vivemos conectados, mas muitas vezes vulneráveis por desconhecimento. Mostrar que segurança digital vai muito além de antivírus é uma missão que carrego comigo e pretendo expandir por meio deste projeto.

Além disso, este trabalho representa minha identidade: curiosidade, ética, responsabilidade digital e paixão por aprender.

# Escopo

Conteúdo do Site:

- Home: Frase de impacto, introdução ao conceito de hacking e cibersegurança.

- Como se Proteger?: Explicações sobre boas práticas de segurança digital.

- Hacking: Tipos de Hackers, motivações e perfis (Black Hat, White Hat, etc.).

- Hardware: Conteúdo sobre dispositivos de Hacking e ferramentas físicas.

- Quiz Segurança: Quiz interativo para testar conhecimentos do usuário.

- Login: Área de autenticação

Design e Experiência do Usuário:

- Vídeo de fundo com estética cyberpunk/matrix.

- Navegação fluida com menu fixo.

- Ícones temáticos em cada seção.

- Tipografia e cores que remetem ao universo hacker (verde, preto, branco).

Tecnologias Utilizadas:

- HTML e CSS para estrutura e estilo.

- JavaScript (parcialmente) para animações e interatividade.

- Futuramente: Node.js para back-end e banco de dados (MYSQL).

# Premissa

- Educação como foco principal: site com propósito educativo, visando conscientizar, informar e capacitar usuários sobre segurança digital.

- Abordagem ética do Hacking: todo o conteúdo relacionado ao Hacking terá caráter instrutivo e ético, destacando o papel de hackers White Hat e desmistificando a figura do hacker criminoso.

- Público-alvo jovem e iniciante: o conteúdo será construído considerando que o público tem pouco ou nenhum conhecimento prévio sobre segurança digital e tecnologia.

- Interação e engajamento como ferramentas de ensino: o projeto utilizará elementos interativos como quizzes, vídeos e simulações para reforçar a experiência de aprendizagem.

- Base técnica escalável: a estrutura do site será desenvolvida inicialmente com HTML, CSS front-end JavaScript, Node.js, MySQL, virtual-box no back-end.

- Responsabilidade digital como valor central: todo o projeto será pautado em princípios de ética, respeito à privacidade, combate a fraudes e uso responsável da tecnologia.

# Restrição

- Sem incentivo ou instrução a práticas ilícitas: nenhum conteúdo poderá ensinar técnicas de invasão real ou disseminação de malwares, nem promover qualquer prática ilegal.

- Privacidade dos usuários: caso o site venha a coletar dados no futuro, deverá seguir boas práticas de proteção de dados, com política de privacidade clara.

# BackLog

- Criar

- Adicionar integração com APIs web-data-viz.

- Incluir criação de senha em tempo real.

- Incluir quizz para treino e aprendizado do usuário.

- Inserir conteúdo sobre Hacking ético.

Bibliografia.

<https://www.open.edu/openlearn/digital-computing/introduction-cyber-security-stay-safe-online/content-section-overvie>

<https://cyberhoot.com/cybrary/cybersecurity>

<https://www.staysafeonline.org/resources/online-safety-and-privacy>

<https://www.ibm.com/think/topics/cybersecurity>

<https://aws.amazon.com/pt/what-is/cybersecurity/>