INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

GUIA PRÁTICO PARA SEGURANÇA DIGITAL

@inccbrasil

www incc.org.br

CARTA DE ABERTURA

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

Caro Leitor,

Nos últimos anos, temos testemunhado um aumento exponencial dos ataques cibernéticos em todo o mundo. Com o avanço da tecnologia, os cibercriminosos têm desenvolvido técnicas cada vez mais sofisticadas para explorar vulnerabilidades e enganar pessoas, organizações e instituições.

A imensa variedade de golpes, crimes e incidentes cibernéticos, incluindo estratégias de engenharia social (levar as pessoas a cometerem erros ou atos contra si mesmos), compromete severamente os governos, as instituições públicas e privadas, assim como o cidadão comum. Isso destaca a necessidade urgente de uma defesa robusta e informada contra essas ameaças.

Neste contexto, é essencial que os servidores públicos, colaboradores da iniciativa privada e cada cidadão brasileiro estejam bem-informados e equipados para enfrentar esses desafios. A segurança cibernética não é apenas uma responsabilidade individual, empresarial ou do poder público, mas uma necessidade coletiva que afeta nossas vidas, nossas informações sensíveis e a segurança de nossas famílias.

Este guia prático de segurança digital é uma iniciativa do Instituto Nacional de Combate ao Cibercrime – INCC, que busca, como uma de suas frentes prioritárias, ampliar o nível de conscientização da sociedade sobre o tema, sendo este o primeiro entre os seis eixos centrais desenvolvidos pela organização para que nosso país possa prosperar na agenda de ampliação da resiliência e maturidade cibernética.

Caso você tenha interesse em conhecer todos os eixos, acesse o relatório completo que traz um panorama detalhado sobre a situação da cibersegurança no Brasil e propostas para a Estratégia Nacional de Cibersegurança clicando **aqui.** Além do relatório completo, você encontrará diversos conteúdos relacionados ao tema.

Compreendendo as diferentes possibilidades e formas de ataque, e implementando medidas básicas de segurança digital, seja em sua vida pessoal ou em seu ambiente de trabalho, fortalecemos não apenas a nossa própria segurança, mas também contribuímos positivamente para a integridade e a confiança em nossas instituições e na própria sociedade.

A segurança cibernética começa com cada um de nós, e juntos podemos construir um ambiente digital mais seguro para todos.

Ótima leitura e se mantenha seguro!

Instituto Nacional de Combate ao Cibercrime

ÍNDICE

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

CAPÍTULO 1

MANTENHA-SE SEGURO NO AMBIENTE DE TRABALHO

A segurança no ambiente de trabalho é um pilar fundamental para a proteção das informações e a continuidade das operações, seja na iniciativa privada ou no poder público. Com a crescente sofisticação dos ataques cibernéticos, torna-se imperativo que todos nós adotemos práticas de segurança robustas e atualizadas. Este capítulo oferece uma orientação básica para os proprietários de pequenas e médias empresas sobre as melhores práticas para proteger seus dados e sistemas no local de trabalho. Estas são as principais questões a serem discutidas com o seu time ou prestadores de serviço de tecnologia.

Primeiramente, o gerenciamento adequado de credenciais (usuários e senhas) é essencial. A criação de senhas fortes e o uso de gerenciadores de senhas (aplicativos no celular) garantem que suas credenciais não sejam facilmente comprometidas. A autenticação multifatorial (MFA) adiciona uma camada extra de segurança, dificultando ainda mais o acesso não autorizado, mesmo que uma senha seja comprometida. **Você já sabe como funciona isso na sua empresa?**

A segurança dos dispositivos em geral também é abordada. A criptografia de disco protege os dados armazenados contra acessos não autorizados, especialmente em caso de perda, roubo ou invasão de dispositivos. Além disso, manter seus dispositivos atualizados com as últimas correções de segurança é crucial para proteger contra vulnerabilidades conhecidas. **Confirme com sua área de T.I se os dados estão criptografados, inclusive de seus dispositivos pessoais.**

O controle de acesso garante que apenas pessoas autorizadas possam acessar as informações, implementando políticas de mínimo privilégio. Ferramentas de gerenciamento de identidade e acesso (IAM) podem ajudar a administrar essas permissões de forma centralizada. **Converse com os técnicos sobre o tema.**

A defesa contra software malicioso é outro aspecto crítico. Soluções de antivírus e técnicas de sandboxing (executar programas suspeitos em um ambiente virtual isolado para identificar malware e testar software) são recomendadas para detectar, prevenir e responder a ameaças, garantindo que aplicativos e arquivos suspeitos sejam isolados e analisados antes de serem executados no sistema principal. **A prevenção é a chave. Ser atacado é uma questão de "quando", e não de "se".**

Ao seguir estas práticas recomendadas e implementá-las de forma consistente, seu ambiente de trabalho será mais seguro e resiliente. Este capítulo serve como um guia dirigido a donos de pequenas e médias empresas que **não entendem de tecnologia**, mas que se **preocupam** em **proteger** seus ativos digitais, atualmente tão ou mais importantes do que os ativos físicos. Cuide da segurança cibernética no seu local de trabalho, protegendo tanto as informações (da sua empresa, funcionários e de clientes) quanto a continuidade do seu negócio. Não se pode mais deixar de olhar para a segurança digital num país tão digitalizado e vulnerável.

GERENCIAMENTO DE CREDENCIAIS (USUÁRIOS E SENHAS)

CRIAÇÃO DE SENHAS FORTES:

Objetivo: Orientação na criação de senhas que sejam seguras e difíceis de serem descobertas.

Implementação: Utilizar uma combinação de letras maiúsculas, minúsculas, números e símbolos. A senha deve ter pelo menos 12 caracteres. Evitar palavras completas, nomes ou datas facilmente associáveis ao usuário.

Dicas: Usar frases como senha ou, ainda, iniciais de uma frase conhecida, incorporando caracteres especiais para aumentar a segurança.

GERENCIADORES DE SENHAS:

Objetivo: Conscientizar sobre a importância do uso de gerenciadores de senhas para armazenar e gerenciar credenciais (usuários e senhas) de forma segura.

Implementação: Esses aplicativos criam, armazenam e preenchem automaticamente senhas complexas para suas contas. As senhas são armazenadas em um cofre criptografado, acessível apenas por uma senha mestra.

Dicas: Escolher gerenciadores bem avaliados, *como LastPass, 1Password* ou *Bitwarden*.

AUTENTICAÇÃO MULTIFATORIAL (MFA):

Objetivo: Adicionar uma camada extra de segurança além da senha.

Implementação: Configurar a MFA para exigir, além da senha, um segundo fator, como um código enviado por SMS, um aplicativo de autenticação (ex.: *Google Authenticator*) ou um dispositivo físico de segurança (ex.: *YubiKey*).

Benefícios: Mesmo que uma senha seja comprometida, o acesso não será possível sem o segundo fator.

SEGURANÇA DE DISPOSITIVOS

CRIPTOGRAFIA DE DISCO:

Objetivo: Proteger as informações armazenadas nos dispositivos contra acesso não autorizado em caso de perda ou roubo do dispositivo.

Implementação: Ativar a criptografia de disco completo em todos os dispositivos eletrônicos, como *BitLocker* para *Windows* e *FileVault* para *macOS*.

Explicação: A criptografia transforma os dados em uma forma ilegível sem a chave correta, que é solicitada na inicialização do dispositivo.

CONTROLE DE ACESSO:

Objetivo: Assegurar que somente pessoas autorizadas tenham acesso a informações.

Implementação: Criar controles baseados em políticas de mínimo privilégio, onde os usuários recebem apenas os acessos necessários para suas funções, nada a mais.

Dicas: Utilizar sistemas de gerenciamento de identidade e acesso (IAM) para administrar permissões de forma centralizada.

ATUALIZAÇÕES DE SEGURANÇA:

Objetivo: Manter os sistemas protegidos contra vulnerabilidades conhecidas, exploradas por softwares e/ou ataques maliciosos.

Implementação: Configurar atualizações automáticas para o sistema operacional e todos os softwares instalados.

Dicas: Realizar verificações regulares de atualizações e aplicá-las imediatamente. Assegurar que as atualizações de segurança sejam priorizadas e implementadas prontamente, preferencialmente de forma automática.

DEFESA CONTRA SOFTWARE MALICIOSO

SOLUÇÕES DE *ENDPOINT*:

Objetivo: Detectar, prevenir e responder a software malicioso que possa comprometer os dispositivos na rede.

Implementação: Instalar e manter software antivírus atualizado, considerando soluções que ofereçam proteção em tempo real e detecção baseada em comportamento.

Benefícios: Proteger contra uma variedade de ameaças, incluindo vírus, *worms*, *trojans* e *ransomware*.

TÉCNICAS DE *SANDBOXING*:

Objetivo: Isolar aplicativos ou arquivos suspeitos para evitar que afetem os sistemas.

Implementação: Executar aplicativos ou arquivos em um ambiente controlado e isolado que simula o sistema operacional principal, mas não permite alterações permanentes no sistema real.

Benefício: Permite testar programas e arquivos em segurança, observando o comportamento sem risco para os dados e sistemas principais.

Estas dicas oferecem orientações básicas e práticas sobre como implementar as medidas de segurança mínimas no ambiente de trabalho, garantindo um melhor nível de proteção para os dispositivos e dados das pequenas e médias empresas, bem como de seus proprietários, colaboradores e clientes.

CAPÍTULO 2

PREVINA-SE CONTRA OS GOLPISTAS

A engenharia social é uma das táticas mais eficazes usadas por criminosos cibernéticos para obter acesso a informações confidenciais. Ao manipular e explorar a confiança e/ou desatenção das pessoas, esses atacantes conseguem burlar até mesmo os sistemas de segurança mais sofisticados. Este capítulo aborda a importância do conhecimento e as estratégias de prevenção contra a engenharia social que devemos adotar.

Neste capítulo, você aprenderá a reconhecer e se proteger contra diferentes tipos de ataques de engenharia social, como ***phishing, spear phishing, pretexting e baiting***. Você entenderá como identificar sinais de tentativas de fraude, como erros gramaticais, solicitações urgentes e links suspeitos, e receberá orientações sobre como verificar a autenticidade de comunicações suspeitas.

Além disso, o capítulo destaca a importância de medidas de segurança comportamental, como treinamentos contínuos e simulações de incidentes. Tais práticas não só aumentam a conscientização individual e coletiva sobre as ameaças cibernéticas, mas também melhoram a capacidade de resposta e mitigação de incidentes de segurança.

A gestão segura de informações sensíveis, tanto digitais quanto físicas, é fundamental para evitar vazamentos e acessos não autorizados. O capítulo também fornece diretrizes sobre o manuseio, armazenamento e descarte seguro de dados confidenciais, utilizando tecnologias como gerenciamento de direitos digitais (DRM) e criptografia.

Ao aplicar as estratégias e práticas apresentadas neste capítulo, você estará melhor preparado para enfrentar as ameaças de engenharia social, protegendo não apenas a si mesmo, mas também sua família e a integridade das operações privadas e públicas.

TÁTICAS DE ENGENHARIA SOCIAL

PHISHING E SPEAR PHISHING:

Objetivo: Educar sobre o reconhecimento e a prevenção de tentativas de *phishing*, uma técnica de engenharia social que usa e-mails ou mensagens fraudulentas para obter informações confidenciais.

Implementação: Identificar sinais de *phishing*, como erros gramaticais, imagens grosseiras, solicitações urgentes e links ou anexos suspeitos.

Dicas: Promover o uso de filtros de e-mail, treinamento regular em segurança e a prática de verificar a autenticidade de solicitações suspeitas por meios independentes.

PRETEXTING E BAITING:

Objetivo: Evitar que criminosos usem informações fabricadas (*pretexting*) ou iscas (*baiting*) para obter acesso a dados pessoais ou corporativos.

Implementação: Desconfiar sempre que algum desconhecido (incluindo técnicos ou o suporte remoto de instituições) solicitar informações pessoais de qualquer tipo, principalmente relacionadas a credenciais (usuários e senhas).

Dicas: Se tiver qualquer desconfiança ou dúvida, não faça nada e não forneça nenhuma informação. Procure os canais oficiais e faça o contato você mesmo.

MEDIDAS DE SEGURANÇA COMPORTAMENTAL:

TREINAMENTO CONTÍNUO:

Objetivo: Implementar um programa de treinamento contínuo para educar e atualizar os proprietários, gestores e funcionários sobre as ameaças de segurança mais recentes e o que fazer caso desconfie que está sendo vítima de tentativa o golpe.

Implementação: Realizar treinamentos frequentes sobre o tema, conversando com as pessoas em seu ambiente de trabalho, incluindo simulações de ataques e avaliações para medir a retenção de conhecimento pelos colaboradores.

Benefícios: Aumentar a conscientização sobre segurança e reduzir a probabilidade de incidentes causados por erro humano.

SIMULAÇÕES DE ATAQUES:

Objetivo: Orientar sobre simulações de ataques de engenharia social para treinar e testar a reatividade dos funcionários em situações controladas.

Implementação: Criar cenários de ataque, como e-mails de *phishing* fictícios ou chamadas telefônicas de *pretexting*, e monitorar como os funcionários respondem.

Dicas: Analisar os resultados das simulações e fornecer feedback construtivo, discutindo o assunto, tirando dúvidas e aplicando ações práticas e constantes de melhoria para incrementar a segurança

GESTÃO SEGURA DE INFORMAÇÕES:

MANUSEIO DE INFORMAÇÕES:

Objetivo: Esclarecer sobre protocolos de manuseio seguro de documentos e dados sensíveis, tanto digitais quanto físicos.

Implementação: Incluir diretrizes sobre como acessar, compartilhar e armazenar informações confidenciais, limitando o acesso com base na necessidade de saber.

Dicas: Utilizar soluções de gerenciamento de direitos digitais (DRM) e outras tecnologias para controlar o acesso e rastrear o uso de documentos sensíveis.

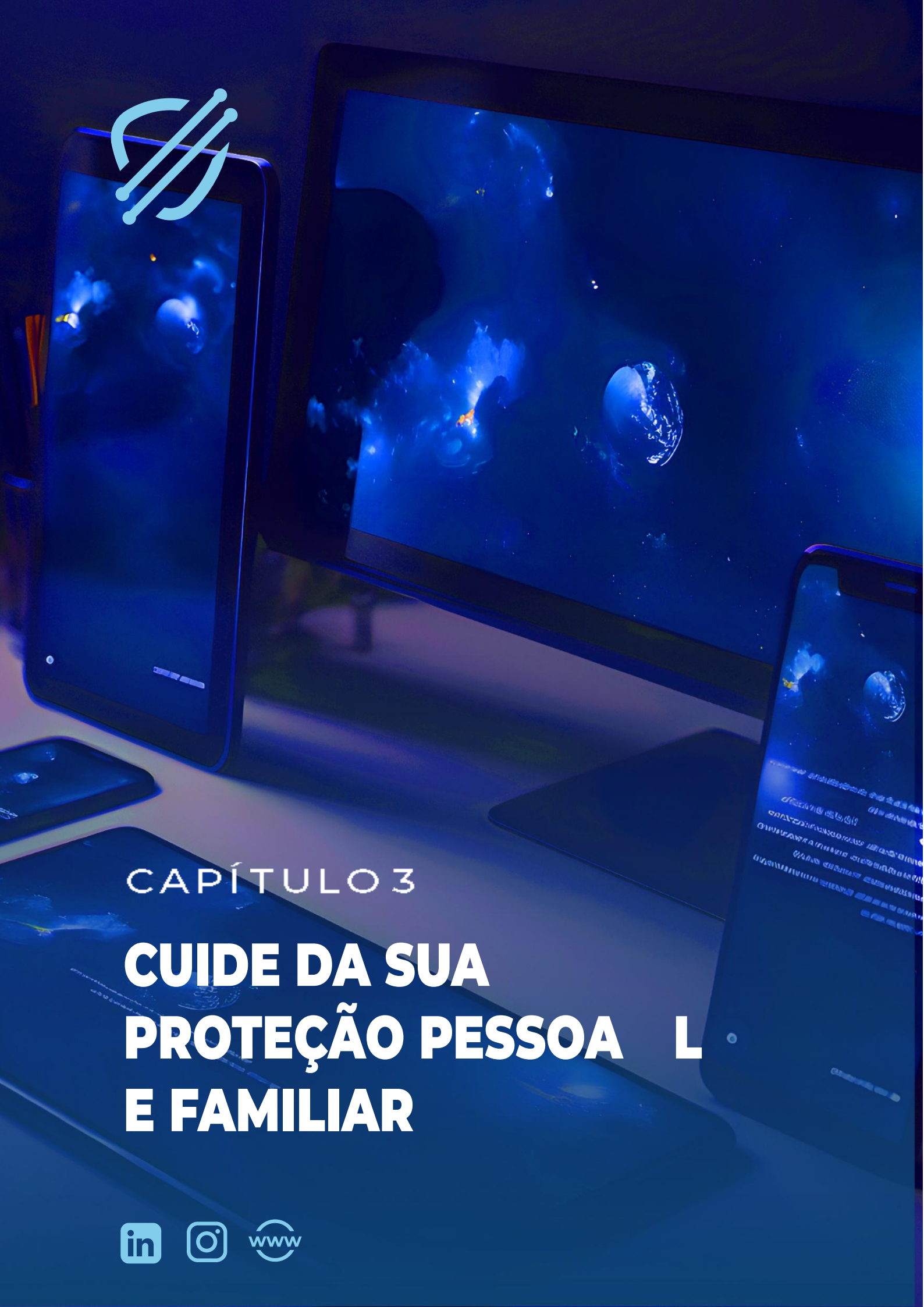
ARMAZENAMENTO E DESCARTE SEGURO:

Objetivo: Garantir que os dados sejam armazenados de forma segura e descartados de maneira adequada quando não forem mais necessários.

Implementação: Utilizar o armazenamento criptografado para informações confidenciais, implementando políticas de acesso mínimo e controlado .

Dicas: Sempre utilizar trituradores de papel para documentos físicos e software de limpeza de dados para mídias digitais, garantindo que as informações não possam ser recuperadas após o descarte ou reutilização do dispositivo por outras pessoas.

Essas práticas são básicas para manter a integridade, disponibilidade e a confidencialidade dos seus dados pessoais ou da empresa.



CAPÍTULO 3

CUIDE DA SUA PROTEÇÃO PESSOAL E FAMILIAR

A segurança cibernética não se limita ao ambiente de trabalho; ela se estende também à proteção pessoal e familiar fora do ambiente de trabalho. Com o aumento das ameaças digitais, é vital que as pessoas adotem medidas para proteger suas informações e dispositivos em todos os aspectos de suas vidas. Este capítulo fornece orientações para melhorar a segurança de dispositivos pessoais e domésticos, bem como para educar e conscientizar as famílias sobre os riscos cibernéticos.

Primeiramente, a segurança de dispositivos móveis, como smartphones e tablets, é fundamental. Este capítulo oferece estratégias para proteger esses dispositivos contra acessos não autorizados e softwares maliciosos, incluindo o uso de códigos de acesso, biometria e aplicativos de segurança. Além disso, recomenda práticas seguras para evitar a exposição a redes Wi-Fi públicas não seguras e a desativação de serviços desnecessários quando não estiverem em uso.

Os dispositivos de Internet das Coisas (IoT), como câmeras de segurança, fechaduras inteligentes e assistentes de voz, também são abordados. Esses dispositivos apresentam vulnerabilidades específicas e conhecidas que podem ser exploradas por criminosos. O capítulo orienta sobre a alteração de senhas padrão (o mais rápido possível), configuração de redes wi-fi separadas para dispositivos *IoT*, assim como orienta a manter os dispositivos atualizados com as últimas atualizações dos fabricantes.

A educação e a conscientização da família são igualmente importantes. Programas de letramento digital familiar, recursos on-line e discussões regulares sobre segurança cibernética ajudam a garantir que todos os membros da família estejam atentos e cientes dos riscos, melhorando a proteção de suas informações e dispositivos. Práticas de gerenciamento de senhas familiares e o uso de *VPNs* para proteger o tráfego da internet também são recomendados.

Ao implementar as medidas de segurança descritas neste capítulo, podemos criar um ambiente mais seguro, tanto em casa quanto no trabalho, protegendo informações pessoais e familiares contra ameaças cibernéticas.

SEGURANÇA DE DISPOSITIVOS PESSOAIS E DOMÉSTICOS

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

PROTEÇÃO DE SMARTPHONES E TABLETS:

Objetivo: Assegurar que dispositivos móveis pessoais sejam protegidos contra acesso não autorizado e malware.

Implementação:

Uso de Códigos de Acesso e Biometria: Implementar bloqueios por senhas seguras, impressão digital ou reconhecimento facial para acesso aos dispositivos.

Atualizações de Segurança: Manter o sistema operacional e os aplicativos sempre atualizados (ative as atualizações automáticas) para proteger contra vulnerabilidades conhecidas.

Instalação de Aplicativos de Segurança: Utilizar aplicativos confiáveis de segurança que ofereçam proteção antivírus e *antimalware*.

Dicas:

Evite conectar-se a redes wi-fi públicas sem proteções adicionais, como a *VPN*.

Desative serviços desnecessários que possam expor o dispositivo a riscos, como *bluetooth* e localização, quando não estiverem em uso.

SEGURANÇA DE *IoT*:

Objetivo: Proteger dispositivos de Internet das Coisas (*IoT*) em casa, como câmeras de segurança, termostatos inteligentes e assistentes de voz, contra invasões e uso malicioso.

Implementação:

Mudança de Senhas Padrão: Substituir todas as senhas padrão de fábrica por senhas fortes e únicas, o mais rápido possível.

Segurança de Rede: Configurar uma rede wi-fi separada especificamente para dispositivos *IoT* para isolá-los do tráfego principal da sua rede doméstica.

Atualizações Regulares: Assegurar que todos os dispositivos *IoT* estejam configurados para receber atualizações automáticas do fabricante.

Dicas:

Informar seus familiares sobre os riscos potenciais associados a dispositivos *IoT* não seguros, como o acesso não autorizado à rede doméstica.

EDUCAÇÃO E CONSCIENTIZAÇÃO DA FAMÍLIA

PROGRAMAS DE EDUCAÇÃO:

Objetivo:

Educar os familiares sobre os riscos cibernéticos e como eles podem proteger suas próprias informações confidenciais e seus dispositivos.

Implementação:

Sessões de Treinamento Familiar: Organizar conversas familiares e informais para discussão de temas como *phishing*, uso seguro da internet e importância das atualizações de segurança e dos backups.

Recursos On-line: Providenciar acesso a cursos on-line e materiais educativos para aprendizagem gratuita e simplificada.

Dicas:

Encoraje discussões regulares sobre segurança cibernética em casa para manter todos informados e conscientes. Debata o tema!

GERENCIAMENTO DE SENHAS:

Objetivo: Promover práticas de gerenciamento de senhas seguras dentro do ambiente familiar.

Implementação:

Uso de Gerenciadores de Senhas: Incentivar a família a usar gerenciadores de senhas para criar e armazenar senhas complexas e únicas.

Educação Sobre Senhas Seguras: Ensinar a importância de senhas fortes e como criar senhas que sejam difíceis de adivinhar ou quebrar.

Não subestimar os atacantes: Converse com seus familiares para que jamais subestimem as capacidades dos atacantes e criminosos.

PRÁTICAS DE NAVEGAÇÃO SEGURA

USO DE *VPNs*:

Objetivo:

Utilizar redes privadas virtuais (*VPNs*) para proteger e criptografar o tráfego da internet, especialmente em redes públicas ou que não sejam confiáveis.

Benefícios:

Proteger dados sensíveis de serem interceptados durante a transmissão entre o seu dispositivo e a internet.

Sempre ocultar a localização real para aumentar a privacidade on-line.

Dicas:

Escolher uma *VPN* confiável, com uma política de não registro de dados e uma forte criptografia. Há muitas opções.

NAVEGADORES E EXTENSÕES SEGURAS:

Objetivo: Melhorar a segurança e a privacidade ao navegar na internet, em especial durante a utilização de navegadores.

CAPÍTULO 4

APRENDA A RESOLVER PROBLEMAS QUE JÁ OCORRERAM

No cenário atual de ameaças cibernéticas, a capacidade de responder rapidamente e recuperar-se eficazmente de incidentes de segurança é essencial. Este capítulo aborda estratégias para preparar, responder e recuperar-se de incidentes cibernéticos (por mais simples que possam ser), garantindo a continuidade da usabilidade e a proteção das informações.

A primeira etapa crucial é o desenvolvimento de um "plano básico de resposta a incidentes". Este plano deve incluir procedimentos claros para a identificação de sinais de incidentes de segurança, como atividades suspeitas na rede, acessos não autorizados e alertas de software de segurança. Ferramentas de monitoramento contínuo e treinamento em reconhecimento de evidências de incidentes são fundamentais para a rápida detecção e atuação.

A comunicação eficiente durante um incidente é importantíssima. Estabelecer com quem falar, o que fazer e como realizar o contato pode fazer toda a diferença (imagine procurar contatos se estiver sem o seu aparelho de celular), mantendo todas as partes interessadas informadas sobre o incidente, sem causar pânico. No caso de empresas, a implementação de ações de contenção, como o isolamento de sistemas infectados e a segmentação da rede, ajudam a limitar a propagação do incidente e a minimizar danos.

A recuperação de dados e sistemas é outra área crítica. Manter backups regulares e criptografados de seus dados sensíveis permite uma recuperação rápida após um incidente. É igualmente importante realizar **testes periódicos de restauração** para garantir que os backups sejam confiáveis e funcionais. Simulações regulares de recuperação utilizando os backups ajudam a testar a eficácia dos planos de recuperação e a fazer ajustes conforme necessário.

Ao adotar as práticas e procedimentos básicos, todos estarão melhor preparados para enfrentar incidentes de segurança, minimizar seus impactos e garantir uma recuperação rápida e eficiente, seja com dados pessoais e/ou empresariais. Acredite, você não desejará descobrir que seus backups não funcionam quando precisar deles. Um dia você certamente precisará! Antecipe-se.

DESENVOLVIMENTO DE UM PLANO DE RESPOSTA A INCIDENTES

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

IDENTIFICAÇÃO DE INCIDENTES:

Objetivo: Ampliar as capacidades e a velocidade de identificação de sinais de um incidente de segurança cibernética.

Implementação:

Monitoramento Contínuo: Implementar ferramentas de monitoramento de rede e sistemas que alertem sobre atividades suspeitas ou anômalas.

Treinamento de Reconhecimento: Educar sobre os sinais comuns de incidentes, como acesso inesperado a arquivos, lentidão na rede e alertas de software de segurança.

Dicas:

Estabelecer um protocolo claro para a comunicação de potenciais incidentes, incluindo quem contatar e como documentar a ocorrência.

COMUNICAÇÃO E CONTENÇÃO:

Objetivo: Assegurar que a comunicação durante um incidente seja eficiente e que as ações de contenção sejam implementadas rapidamente para minimizar danos.

Implementação:

Cadeia de Comando: Definir uma cadeia de comando clara para comunicação durante um incidente, incluindo contatos internos e externos.

Comunicação Transparente: Manter todas as partes interessadas informadas sobre o status do incidente de forma clara e sem provocar pânico.

Dicas:

Implementar o isolamento do sistema ou a segmentação de rede para limitar a propagação do incidente.

Desconectar sistemas infectados da rede para prevenir a disseminação de malware.

RECUPERAÇÃO DE DADOS E SISTEMAS

BACKUPS CRIPTOGRAFADOS:

Objetivo: Manter backups regulares e seguros para permitir a rápida recuperação de dados após um incidente.

Implementação:

Frequência e Tipo: Realizar backups diários, semanais e mensais para diferentes tipos de dados, garantindo que eles sejam armazenados em locais seguros e acessíveis.

Criptografia: Assegurar que todos os backups sejam criptografados para proteger a integridade e a confidencialidade dos dados.

Dicas:

Periodicamente testar a restauração de dados de backups para garantir que sejam confiáveis e estejam funcionando corretamente.

TESTES DE RECUPERAÇÃO:

Objetivo: Garantir que os planos de recuperação sejam eficazes e estejam prontos para serem implementados quando necessário.

Implementação:

Simulações de Recuperação: Realizar simulações regulares de recuperação utilizando os backups para testar a eficácia dos planos de recuperação.

Avaliação e Ajustes: Após cada teste, avaliar a eficiência do processo de recuperação e fazer ajustes conforme necessário para melhorar a resposta a futuros incidentes.

Este capítulo fornece uma base mínima para desenvolver, implementar e manter estratégias eficazes de resposta a incidentes e recuperação de dados. As práticas e procedimentos detalhados ajudarão a minimizar o impacto de incidentes de segurança, garantindo uma recuperação rápida e eficiente.

CAPÍTULO 5

CUIDE DA SEGURANÇA DE SEUS DISPOSITIVOS MÓVEIS

Em um mundo cada vez mais conectado, a segurança de dispositivos móveis é uma prioridade fundamental para cada um de nós, assim como para nossas famílias. Este capítulo oferece diretrizes sobre como proteger smartphones e tablets, dispositivos que são frequentemente alvos de ataques cibernéticos devido ao seu uso extensivo e à quantidade de informações sensíveis que armazenam.

Primeiramente, é essencial manter os dispositivos móveis atualizados com as últimas correções de segurança. Configurar atualizações automáticas garante que o sistema operacional e os aplicativos estejam protegidos contra vulnerabilidades recém-descobertas. O capítulo também aborda a configuração de medidas de segurança biométricas, como *Touch ID* e *Face ID*, para reforçar a proteção dos dispositivos.

A criptografia de dados é outro aspecto crucial. Tanto dispositivos *iOS* quanto *Android* oferecem opções de criptografia que devem ser habilitadas para garantir que os dados armazenados sejam inacessíveis a terceiros em caso de perda ou roubo do dispositivo. Ferramentas como "*Find My iPhone*" e "*Find My Mobile*" também são destacadas, permitindo localizar, bloquear ou apagar remotamente um dispositivo perdido ou roubado.

Além disso, o capítulo discute a importância de utilizar senhas alfanuméricas fortes e gerenciadores de senhas para proteger contas e aplicativos. A ativação de autenticação multifatorial (MFA) é recomendada para adicionar uma camada extra de segurança ao acessar contas e serviços on-line.

A segurança dos dispositivos móveis deve ser estendida a todos, especialmente aos jovens e idosos. O capítulo fornece orientações sobre como treinar membros da família sobre práticas seguras de uso de dispositivos móveis, incluindo a configuração de backups automáticos e a conscientização sobre os riscos de conectar-se a redes wi-fi públicas.

Ao seguir as práticas recomendadas neste capítulo, podemos maximizar a proteção de nossos dispositivos móveis, melhorando a segurança de nossas informações pessoais e sensíveis em todos os momentos.

SEGURANÇA EM DISPOSITIVOS *iOS* (*iPhone*)

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

ATUALIZAÇÕES DE SISTEMA:

Objetivo: Manter o dispositivo atualizado com as últimas correções de segurança.

Implementação:

Navegar até Ajustes > Geral > Atualização de Software.

Habilitar Atualizações Automáticas para receber e instalar atualizações de software automaticamente.

CONFIGURAÇÃO DE *TOUCH ID/Face ID*:

Objetivo: Implementar medidas biométricas para reforçar a segurança.

Implementação:

Ir para Ajustes > *Touch ID* & Código ou *Face ID* & Código.

Configurar a impressão digital ou o reconhecimento facial e ativar o desbloqueio do *iPhone* e autenticação para compras.

ENCRIPTAÇÃO DE DADOS:

Objetivo: Proteger informações pessoais armazenadas no dispositivo.

Implementação:

A criptografia é habilitada automaticamente ao definir um código de acesso em Ajustes > *Touch ID* & Código ou *Face ID* & Código.

FIND MY IPHONE (BUSCA):

Objetivo: Localizar e proteger o *iPhone* em caso de perda ou roubo.

Implementação:

Acessar Ajustes > [seu nome] > *iCloud* > Buscar.

Ativar Buscar *iPhone* para localizar, bloquear ou apagar o dispositivo remotamente.

TEMPO DE USO PARA APLICATIVOS:

Objetivo: Controlar e limitar o uso de aplicativos específicos, configurando senhas para acessá-los.

Implementação:

Acessar Ajustes > Tempo de Uso.

Configurar Restrições de Conteúdo e Privacidade, introduzindo um código que será necessário para fazer mudanças. Em seguida, configurar limites específicos para cada aplicativo conforme desejado.

PROTEÇÃO CONTRA ROUBO:

Objetivo: Reforçar a segurança do dispositivo em caso de roubo.

Implementação:

Utilizar *Find My iPhone* e habilitar o Modo Perdido, que bloqueia o dispositivo com uma senha e mostra uma mensagem personalizada na tela de bloqueio.

SENHAS ALFANUMÉRICAS:

Objetivo: Fortalecer a segurança do dispositivo usando uma senha mais complexa que combina letras, números e símbolos.

Implementação:

Ir para Ajustes > *Touch ID* & Código ou *Face ID* & Código e selecionar Alterar Código.

Escolher a opção Opções de Código e selecionar Código Alfanumérico Personalizado.

Inserir uma senha que combine letras (maiúsculas e minúsculas), números e símbolos para criar uma barreira robusta contra tentativas de acesso não autorizado.

SEGURANÇA EM DISPOSITIVOS *ANDROID (SAMSUNG)*

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

ATUALIZAÇÕES DE SISTEMA:

Objetivo: Garantir que o dispositivo esteja protegido contra vulnerabilidades recentemente descobertas.

Implementação:

Ir para Configurações > Atualização de software e ativar baixar e instalar automaticamente.

CONFIGURAÇÃO *DE SCREEN LOCK:*

Objetivo: Proteger o dispositivo com um método de desbloqueio seguro.

Implementação:

Acessar Configurações > Tela de bloqueio > Tipo de tela de bloqueio e escolher entre padrão, *PIN*, senha ou biometria.

ENCRIPTAÇÃO DE DADOS:

Objetivo: Assegurar que os dados pessoais não sejam acessíveis em caso de acesso não autorizado ao dispositivo.

Implementação:

Verificar em Configurações > Segurança > Criptografar dispositivo, garantindo que a criptografia esteja ativa.

FIND MY MOBILE (PARA SAMSUNG):

Objetivo: Capacidade de localizar, bloquear ou apagar seu dispositivo remotamente.

Implementação:

Ir para Configurações > Biometria e segurança > Encontrar meu celular e ativar as opções relevantes, incluindo 'Controle remoto' e 'Enviar última localização'.

SENHAS ALFANUMÉRICAS:

Objetivo: Aumentar significativamente a segurança do dispositivo com uma senha forte.

Implementação:

Acessar Configurações > Tela de bloqueio > Tipo de tela de bloqueio > Senha.

Definir uma senha que inclua uma mistura de letras (maiúsculas e minúsculas), números e, se desejado, símbolos.

ORIENTAÇÕES PARA FAMÍLIARES

TREINAMENTO DE SEGURANÇA:

Objetivo: Instruir cônjuges e filhos sobre práticas seguras de uso de dispositivos móveis.

Implementação:

Realizar sessões educativas sobre segurança digital, abordando temas como *phishing*, navegação segura e o significado das permissões de aplicativos.

PRÁTICAS RECOMENDADAS PARA TODOS OS USUÁRIOS:

Implementação:

Ensinar a configurar backups automáticos para fotos, contatos e dados importantes.

Dicas:

Aconselhar sobre a instalação de aplicativos apenas de fontes confiáveis e rever as permissões solicitadas antes da instalação.

CAPÍTULO 6

APRENDA A PROTEGER SUAS REDES SOCIAIS

As redes sociais desempenham um papel central na comunicação e na interação moderna, mas também apresentam riscos significativos de segurança. Este capítulo explora os principais riscos associados às plataformas de redes sociais e oferece estratégias para mitigá-los, protegendo as informações pessoais e profissionais de todos.

Com bilhões de usuários em todo o mundo, redes sociais como *Facebook, Instagram, Twitter, LinkedIn, Snapchat e TikTok* são alvos atraentes para criminosos cibernéticos. Eles utilizam essas plataformas para conduzir ataques de *phishing*, espalhar desinformação, cometer fraudes e realizar crimes on-line. Este capítulo detalha as características de cada plataforma, destacando suas vulnerabilidades específicas e como os usuários podem se proteger.

Uma das medidas de segurança mais eficazes é a ativação da autenticação multifatorial (MFA). Ao exigir um segundo fator de autenticação além da senha, os usuários podem adicionar uma camada extra de proteção contra acessos não autorizados. O capítulo também recomenda a revisão regular das atividades de login e a configuração de opções de segurança adicionais, como contatos de confiança e notificações de segurança.

A privacidade é outro aspecto crucial. Ajustar as configurações de privacidade nas redes sociais para limitar a exposição de informações pessoais pode reduzir significativamente os riscos. O capítulo fornece orientações passo a passo sobre como configurar essas opções em cada plataforma, ajudando os usuários a controlarem quem pode ver suas informações e interagir com elas.

Além das configurações de privacidade, o comportamento seguro nas redes sociais é essencial. Evitar a divulgação excessiva de informações pessoais e locais que frequenta, ser cauteloso ao clicar em links ou baixar anexos de fontes desconhecidas e verificar a autenticidade de solicitações e mensagens suspeitas são práticas recomendadas.

FACEBOOK

CARACTERÍSTICAS:

Maior plataforma de rede social do mundo, oferecendo recursos de compartilhamento de conteúdo, mensagens, grupos e páginas.

OBJETIVOS:

Facilitar a conexão e interação entre amigos, família e comunidades.

USOS COMUNS:

Compartilhamento de fotos, vídeos, status de vida, notícias e eventos.

PRINCIPAIS RISCOS:

Exposição excessiva de informações pessoais, *phishing*, disseminação de desinformação e conteúdo nocivo.

FALHAS DE SEGURANÇA:

Vulnerabilidades de privacidade, incluindo configurações de privacidade confusas e falhas de proteção de dados.

OPÇÕES DE SEGURANÇA ADICIONAIS:

Verificação em Duas Etapas:

Acesse Configurações > Segurança e *Login*.

Em "Usar autenticação de dois fatores", clique em "Editar".

Escolha o método de autenticação desejado (como SMS ou um aplicativo de autenticação).

Siga as instruções para concluir a configuração.

Revisão de Atividades de Login:

Vá para Configurações > Segurança e *Login*.

Em "Onde você está conectado", clique em "Ver mais".

Revise as sessões ativas e desconecte aquelas que parecem suspeitas.

Contatos de Confiança:

Acesse Configurações > Segurança e *Login*.

Em "Contatos de confiança", clique em "Editar".

Adicione os contatos que você confia para ajudar a recuperar sua conta, se necessário.

INSTAGRAM

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

CARACTERÍSTICAS:

Plataforma de compartilhamento de fotos e vídeos com recursos de edição e filtros.

OBJETIVOS:

Compartilhar momentos do dia a dia de forma visualmente atraente e inspiradora.

USOS COMUNS:

Postagem de fotos e vídeos, interação com publicações de amigos e influenciadores.

PRINCIPAIS RISCOS:

Exposição excessiva de estilo de vida, *cyberbullying*, vazamento de fotos privadas.

FALHAS DE SEGURANÇA:

Vulnerabilidades de privacidade, como configurações de conta padrão que podem expor informações pessoais.

OPÇÕES DE SEGURANÇA ADICIONAIS:

Atividade da Conta:

Vá para Configurações > Segurança.

Em "Segurança", clique em "Ver todas as atividades de *login*".

Revise a atividade recente e desconecte as sessões suspeitas.

Autenticação de Dois Fatores:

Acesse Configurações > Segurança.

Em "Autenticação de dois fatores", toque em "Autenticar".

Selecione o método de autenticação preferido e siga as instruções para configurar.

TWITTER

CARACTERÍSTICAS:

Plataforma de *microblogging* que permite postagens curtas de até 280 caracteres.

OBJETIVO:

Compartilhar pensamentos, notícias e opiniões de forma rápida e concisa.

USOS COMUNS:

Compartilhamento de atualizações pessoais, engajamento em debates e discussões públicas.

PRINCIPAIS RISCOS:

Disseminação de desinformação, assédio on-line, exposição a conteúdo ofensivo.

FALHAS DE SEGURANÇA:

Vulnerabilidades de *phishing*, contas comprometidas devido a senhas fracas ou reutilizadas.

OPÇÕES DE SEGURANÇA ADICIONAIS:

Verificação em Duas Etapas:

Acesse Configurações e Privacidade > Segurança e Conta.

Em "Segurança", encontre "Verificação em duas etapas" e ative-a.

Siga as instruções para configurar a verificação em duas etapas.

Atividade da Conta:

Vá para Configurações e Privacidade > Conta.

Em "Dados e Permissões", clique em "Atividade da conta".

Revise a atividade recente e desconecte as sessões suspeitas.

LINKEDIN

CARACTERÍSTICAS:

Rede social profissional focada em *networking* e oportunidades de carreira.

OBJETIVO:

Facilitar a conexão entre profissionais, recrutamento e compartilhamento de conhecimento.

USOS COMUNS:

Construção de perfil profissional, busca de emprego, compartilhamento de artigos e insights de negócios.

PRINCIPAIS RISCOS:

Roubo de identidade profissional, *phishing* direcionado a profissionais, exposição a golpes de recrutamento falsos.

FALHAS DE SEGURANÇA:

Vulnerabilidades de privacidade, como informações pessoais e histórico de emprego sendo compartilhados publicamente.

OPÇÕES DE SEGURANÇA ADICIONAIS:

Verificação de *Login*:

Vá para Configurações de Privacidade e Segurança > Acesso e Segurança.

Em "Verificação de *Login*", clique em "Ativar".

Siga as instruções para configurar a verificação de *login*.

SNAPCHAT

CARACTERÍSTICAS:

Plataforma de mensagens efêmeras que permite o envio de fotos e vídeos que desaparecem após visualizados.

OBJETIVO:

Facilitar conversas e compartilhamento de momentos espontâneos e autênticos.

USOS COMUNS:

Compartilhamento de *selfies*, vídeos engraçados, atualizações rápidas sobre o dia a dia.

PRINCIPAIS RISCOS:

Vazamento de fotos privadas, *cyberbullying*, acesso indevido a conteúdo efêmero.

FALHAS DE SEGURANÇA:

Histórico de vulnerabilidades de privacidade, como vazamentos de dados de usuários e falhas na segurança de mensagens.

OPÇÕES DE SEGURANÇA ADICIONAIS:

Localização Fantasma:

Toque no ícone de perfil no canto superior esquerdo da tela.

Vá para Configurações > Ver minha localização.

Selecione "Localização Fantasma" para ocultar sua localização dos amigos.

TIKTOK

CARACTERÍSTICAS:

Plataforma de mídia social de compartilhamento de vídeos curtos.

OBJETIVOS:

Criar e compartilhar vídeos de entretenimento, dança, comédia e educação.

USOS COMUNS:

Criação de vídeos criativos, desafios virais, compartilhamento de tendências.

PRINCIPAIS RISCOS:

Exposição a conteúdo inadequado, coleta excessiva de dados, riscos de segurança devido a práticas de segurança insuficientes.

FALHAS DE SEGURANÇA:

Relatórios de coleta de dados de usuários, exposição a conteúdo inapropriado, privacidade de dados inadequada.

OPÇÕES DE SEGURANÇA ADICIONAIS:

Conta Privada:

Acesse o seu perfil e clique nos três pontos no canto superior direito.

Selecione "Privacidade e Segurança".

Ative "Conta Privada" para que apenas seguidores aprovados possam ver seus vídeos.

CAPÍTULO 7

PROTEJA SEUS SERVIÇOS DE ARMAZANAMENTO EM NUVEM

O armazenamento em nuvem transformou a maneira como armazenamos, acessamos e compartilhamos dados, oferecendo conveniência e acessibilidade. No entanto, a segurança desses dados é uma preocupação crítica, especialmente para servidores públicos e privados que lidam com informações sensíveis. Este capítulo explora as melhores práticas para garantir a segurança no uso de serviços de armazenamento em nuvem.

Com diversas opções disponíveis, como *Google Drive, Dropbox, Microsoft OneDrive* e *iCloud*, é essencial entender as características de segurança de cada plataforma. Este capítulo detalha os níveis de segurança oferecidos por esses serviços, incluindo criptografia de dados em trânsito e em repouso, controle de acesso e autenticação multifatorial (MFA).

Ao escolher um serviço de armazenamento em nuvem, deve-se considerar não apenas a segurança, mas também a integração com outros serviços e dispositivos. Por exemplo, o *Google Drive* se integra bem com outros serviços do *Google*, enquanto o *Microsoft OneDrive* oferece uma integração perfeita com o ecossistema *Microsoft*. O capítulo fornece uma análise comparativa de cada serviço, destacando seus prós e contras para ajudar os usuários a fazerem escolhas informadas.

Além disso, o capítulo oferece orientações sobre como configurar e utilizar esses serviços de forma segura. Isso inclui a definição de permissões de acesso adequadas, a implementação de backups regulares e a ativação de notificações de atividades suspeitas. A educação sobre a importância de utilizar senhas fortes e únicas para contas de armazenamento em nuvem também é enfatizada.

Ao adotar as práticas de segurança descritas neste capítulo, podemos proteger melhor nossos dados armazenados na nuvem, garantindo que informações sensíveis permaneçam seguras contra acessos não autorizados e outras ameaças cibernéticas.

GOOGLE DRIVE

CARACTERÍSTICAS:

Integração com serviços do *Google*, como *Gmail* e *Google* Fotos.

Capacidade de criar, editar e compartilhar documentos do *Google Docs*, *Sheets* e *Slides*.

Planos gratuitos e pagos disponíveis com diferentes capacidades de armazenamento.

NÍVEL DE SEGURANÇA:

Criptografia de dados em trânsito e em repouso.

Controle de acesso granular para arquivos e pastas.

PRÓS:

Integração com outros serviços do *Google*.

Facilidade de uso e colaboração em tempo real.

CONTRAS:

Privacidade pode ser uma preocupação devido à coleta de dados pelo *Google*.

COMO ESCOLHER:

Ideal para usuários que já utilizam outros serviços do *Google* e precisam de colaboração em equipe.

DROPBOX

CARACTERÍSTICAS:

Fácil compartilhamento de arquivos e colaboração em equipe.

Sincronização automática de arquivos em todos os dispositivos.

Planos gratuitos e pagos com opções de armazenamento flexíveis.

NÍVEL DE SEGURANÇA:

Criptografia de dados em trânsito e em repouso.

Recuperação de versões anteriores de arquivos.

PRÓS:

Interface simples e intuitiva.

Ótimo para compartilhar arquivos grandes.

CONTRAS:

Planos pagos podem ser caros para armazenamento adicional.

COMO ESCOLHER:

Recomendado para usuários individuais e equipes que valorizam a simplicidade e a facilidade de uso.

MICROSOFT ONEDRIVE

CARACTERÍSTICAS:

Integração com o *Microsoft Office* para edição de documentos on-line.

Armazenamento automático de fotos do dispositivo móvel.

Oferece planos gratuitos e pagos com opções de armazenamento expansíveis.

NÍVEL DE SEGURANÇA:

Criptografia de dados em trânsito e em repouso.

Controles de compartilhamento granular para arquivos e pastas.

PRÓS:

Integração perfeita com o *Office* e o *Windows*.

Excelente para usuários que dependem do ecossistema *Microsoft*.

CONTRAS:

A interface pode ser um pouco confusa para alguns usuários.

COMO ESCOLHER:

Indicado para usuários que usam ativamente produtos *Microsoft* e precisam de integração perfeita.

ICLOUD (PARA USUÁRIOS *APPLE*)

CARACTERÍSTICAS:

Integração perfeita com dispositivos *Apple*.

Armazenamento de backups de dispositivos *iOS*.

Compartilhamento familiar permite compartilhar compras e armazenamento com até seis membros da família.

NÍVEL DE SEGURANÇA:

Criptografia de ponta a ponta para dados armazenados.

Autenticação de dois fatores para proteger a conta.

PRÓS:

Integração nativa com dispositivos *Apple*.

Backup automático e fácil de dispositivos *iOS*.

CONTRAS:

Capacidade limitada de armazenamento gratuito.

COMO ESCOLHER:

Melhor para usuários que possuem dispositivos *Apple* e desejam uma integração perfeita entre dispositivos.

Ao escolher um serviço de armazenamento em nuvem, considere suas necessidades específicas, preferências de integração com outros serviços e dispositivos, e o nível de segurança oferecido por cada provedor. Opte pelo serviço que melhor atenda às suas necessidades e ofereça os recursos de segurança adequados para proteger seus dados pessoais.

CAPÍTULO 8

CUIDE DA SEGURANÇA DOS DISPOSITIVOS DA SUA CASA

A crescente adoção de dispositivos de Internet das Coisas (*IoT*) transformou residências e cidades em ambientes conectados e inteligentes. Contudo, esses dispositivos — como câmeras de segurança, fechaduras inteligentes e assistentes de voz — também introduzem novas vulnerabilidades que podem ser exploradas por cibercriminosos. Este capítulo aborda as principais ameaças associadas aos dispositivos *IoT* e oferece estratégias para proteger a segurança residencial.

Os dispositivos *IoT* podem ser alvos fáceis se não forem configurados corretamente. Senhas padrão fracas, falta de atualizações de firmware e configurações de acesso remoto não autorizadas são algumas das vulnerabilidades comuns. Aqui, orientamos sobre como mitigar esses riscos, começando pela alteração imediata de senhas padrão para senhas fortes e únicas, além da manutenção regular de atualizações de firmware para corrigir vulnerabilidades conhecidas.

A segurança da rede é outro aspecto crítico. Configurar uma rede wi-fi separada exclusivamente para dispositivos *IoT* pode isolar esses aparelhos do tráfego principal da rede doméstica, reduzindo o risco de comprometimento. A ativação da autenticação multifatorial (MFA) e a configuração de roteadores para permitir apenas dispositivos autorizados são práticas recomendadas.

Além disso, é importante desativar serviços e recursos não utilizados, como câmeras e microfones, quando não estiverem em uso. Isso pode prevenir o acesso não autorizado e proteger a privacidade dos moradores. O monitoramento regular do uso de dados e a revisão das permissões de aplicativos também são essenciais para identificar e mitigar possíveis ameaças.

A segurança dos dispositivos *IoT* é uma responsabilidade contínua. Manter-se informado sobre as melhores práticas e seguir as orientações dos fabricantes pode ajudar a proteger sua casa e sua família contra ameaças cibernéticas. Ao implementar as estratégias descritas neste capítulo, garantimos que nossas residências inteligentes sejam mais seguras e resilientes.

CÂMERAS DE SEGURANÇA Wi-Fi

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

VULNERABILIDADES POTENCIAIS:

Senhas Padrão Fracas: Muitas câmeras vêm com senhas padrão facilmente descobertas por hackers.

Falta de Atualizações de Firmware: Dispositivos desatualizados podem ter vulnerabilidades conhecidas.

Acesso Remoto Não Autorizado: Configurações incorretas podem permitir acesso não autorizado às câmeras pela internet.

PROTEÇÕES DISPONÍVEIS:

Alteração de Senha Padrão: Sempre altere a senha padrão para uma senha forte e única.

Atualizações de *Firmware*: Verifique regularmente se há atualizações do fabricante e instale-as assim que disponíveis.

Autenticação de Dois Fatores: Ative a autenticação de dois fatores para uma camada adicional de segurança.

SMART TVs

VULNERABILIDADES POTENCIAIS:

Coleta de Dados Pessoais: Algumas TVs inteligentes podem coletar dados de visualização sem consentimento explícito do usuário.

Vulnerabilidades de Sistema Operacional: Sistemas desatualizados podem ser vulneráveis a ataques.

Acesso Não Autorizado à Câmera e ao Microfone: Hackers podem explorar falhas para acessar dispositivos de áudio e vídeo.

PROTEÇÕES DISPONÍVEIS:

Controle de Privacidade: Desative a coleta de dados quando possível e verifique as configurações de privacidade da TV.

Atualizações de Software: Mantenha o software da TV atualizado para proteger contra vulnerabilidades conhecidas.

Desligamento de Microfone e Câmera: Desative recursos de áudio e vídeo quando não estiverem em uso para proteger a privacidade.

TERMOSTATOS INTELIGENTES

VULNERABILIDADES POTENCIAIS:

Acesso Remoto Não Autorizado: Senhas fracas podem permitir acesso não autorizado ao termostato.

Vulnerabilidades de Segurança no Aplicativo: Aplicativos mal protegidos podem ser alvos de ataques.

Coleta de Dados Sensíveis: Termostatos inteligentes podem coletar informações sobre os hábitos domésticos dos usuários.

PROTEÇÕES DISPONÍVEIS:

Configurações de Segurança do Aplicativo: Verifique se o aplicativo do termostato possui configurações de segurança adequadas, como autenticação de dois fatores.

Atualizações de *Firmware*: Mantenha o *firmware* do termostato atualizado para corrigir vulnerabilidades conhecidas.

Monitoramento de Uso de Dados: Revise e ajuste as permissões de dados concedidas ao termostato.

FECHADURAS INTELIGENTES

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

VULNERABILIDADES POTENCIAIS:

Senhas Fracas ou Compartilhadas: Senhas fáceis de adivinhar podem comprometer a segurança da fechadura.

Acesso Remoto Não Autorizado: Configurações inadequadas podem permitir que hackers controlem a fechadura remotamente.

Vulnerabilidades no Aplicativo Móvel: Aplicativos mal protegidos podem ser alvos de ataques.

PROTEÇÕES DISPONÍVEIS:

Senhas Fortes e Únicas: Use senhas fortes e exclusivas para acessar o aplicativo e controlar a fechadura.

Controle de Acesso Remoto: Limite o acesso remoto apenas a dispositivos confiáveis e redes seguras.

Verificação de Registro de Acesso: Monitore regularmente o registro de acesso e verifique atividades suspeitas.

Ao utilizar dispositivos *IoT* em casa, é crucial implementar medidas de segurança adequadas para proteger sua privacidade e segurança. Mantenha-se informado sobre as melhores práticas e siga as orientações do fabricante para garantir que seus dispositivos permaneçam atualizados e seguros.

CAPÍTULO 9

APRENDA A IDENTIFICAR GOLPES

Com a evolução constante da tecnologia, os ataques cibernéticos tornaram-se mais sofisticados e variados. Conhecer os diferentes tipos de ataques e saber como identificá-los é crucial para proteger as informações e garantir a segurança cibernética. Este capítulo oferece uma visão geral dos principais tipos de ataques cibernéticos e as melhores práticas para reconhecê-los e preveni-los.

Os ataques de *phishing* são uma das formas mais comuns de engenharia social, onde os atacantes enviam e-mails ou mensagens fraudulentas que parecem vir de fontes confiáveis. Este capítulo explica como reconhecer sinais de *phishing*, como endereços de e-mail suspeitos, solicitações de informações pessoais não solicitadas e links para sites falsos.

Outro tipo significativo de ameaça é o *malware*, que inclui vírus, *ransomware*, *spyware* e cavalos de Troia. O capítulo aborda como identificar sinais de infecção por *malware*, como lentidão do sistema, *pop-ups* frequentes e arquivos ou programas inesperados. Manter o software antivírus atualizado e realizar varreduras regulares são práticas recomendadas para proteger-se contra essas ameaças.

Os ataques de engenharia social exploram a confiança e a manipulação psicológica para obter informações confidenciais ou induzir ações prejudiciais. Este capítulo aborda técnicas como *pretexting* e *baiting*, fornecendo exemplos práticos e estratégias de defesa, como a verificação da identidade dos solicitantes e a conscientização sobre táticas de manipulação.

Os ataques de força bruta, que tentam adivinhar senhas repetidamente, também são discutidos. Implementar senhas fortes e únicas, monitorar atividades de *login* e ativar a autenticação multifatorial são métodos eficazes para se proteger contra esses ataques.

O *ransomware*, que criptografa arquivos de um sistema e exige um resgate para desbloqueá-los, é outra ameaça crítica. Este capítulo explica como identificar uma infecção por *ransomware* e a importância de manter backups regulares e criptografados dos dados.

Compreender os diferentes tipos de ataques cibernéticos e aplicar as práticas de segurança descritas neste capítulo pode melhorar significativamente nossa capacidade de identificar e mitigar essas ameaças, protegendo nossas informações e garantindo a continuidade das operações pessoais e profissionais.

PHISHING

Descrição: O *phishing* envolve o envio de e-mails ou mensagens falsas que parecem ser de fontes legítimas, com o objetivo de induzir os usuários a revelar informações pessoais, como senhas e números de cartão de crédito.

Evidências:

Endereços de e-mail suspeitos.

Solicitações de informações pessoais não solicitadas.

Links para sites falsos.

Como Identificar: Verifique sempre o remetente do e-mail, examine cuidadosamente os links e nunca compartilhe informações pessoais em resposta a solicitações não solicitadas.

MALWARE

Descrição: O *malware* é um software malicioso projetado para danificar ou controlar um sistema sem o consentimento do usuário. Isso inclui vírus, *ransomware*, *spyware* e cavalos de Troia.

Evidências:

Computador ou dispositivo mais lento que o normal.

Pop-ups ou mensagens de erro frequentes.

Arquivos ou programas inesperados.

Como Identificar: Mantenha seu software antivírus atualizado, evite clicar em links ou fazer download de arquivos de fontes desconhecidas e faça varreduras regulares em seu sistema.

ENGENHARIA SOCIAL

Descrição: A engenharia social envolve manipular as pessoas para que divulguem informações confidenciais ou realizem ações prejudiciais, muitas vezes através de técnicas de persuasão.

Evidências:

Pedidos de informações confidenciais por telefone ou e-mail.

Ofertas muito boas para serem verdadeiras.

Manipulação emocional para induzir ações específicas.

Como Identificar: Esteja sempre ciente de quem está solicitando informações pessoais e pense duas vezes antes de agir com base em solicitações incomuns ou suspeitas.

DEEP FAKES (ÁUDIO E VÍDEO)

Descrição:

Um *deepfake* é uma técnica de manipulação de mídia (principalmente vídeos e áudios) que usa inteligência artificial para criação de conteúdos falsos e realistas. Com ela, é possível "trocar" o rosto ou a voz de uma pessoa por outra em um vídeo ou áudio, fazendo parecer que alguém está dizendo ou fazendo algo que nunca fez.

Evidências:

Um olhar mais atento é a chave para desconfiar de deepfakes. Preste atenção em movimentos faciais incomuns, Sincronização labial falha (entre a fala e o movimento labial), Iluminação inconsistente, Pele e textura irrealistas, Pistas auditivas (voz metalizada) e Interação irreal com objetos, entre outras falhas que podem chamar a atenção. Mensagens de ódio e extremismo também devem despertar sua atenção, em especial quando envolvem figuras públicas.

RANSOMWARE

Descrição:

O *ransomware* é um tipo de *malware* que criptografa os arquivos de um sistema e exige um resgate para desbloqueá-los. Os criminosos normalmente ameaçam destruir os arquivos se o resgate não for pago.

Evidências:

Mensagens de resgate exigindo pagamento em criptomoeda.

Arquivos bloqueados com extensões incomuns.

Mensagens de alerta informando sobre a infecção por *ransomware*.

Prevenção:

Mantenha backups regulares de seus arquivos importantes, mantenha seu software antivírus atualizado e evite clicar em links ou fazer download de anexos de e-mails suspeitos.

Ao estar ciente dos diferentes tipos de ataques cibernéticos e suas características, podemos tomar medidas proativas para proteger nossa segurança e privacidade on-line. Permanecer informado sobre as melhores práticas de segurança cibernética e estar atento a atividades suspeitas são fundamentais para uma experiência on-line segura.

CAPÍTULO 10

PROTEJA SUA VIDA FINANCEIRA

Realizar transações financeiras nunca foi tão fácil e rápido, graças aos avanços da tecnologia e à crescente popularidade dos aplicativos e serviços on-line. Essa conveniência traz muitos benefícios, permitindo que você gerencie suas finanças com apenas alguns toques na tela. No entanto, é crucial estar ciente dos riscos associados a essas transações e adotar medidas de segurança para proteger suas informações financeiras.

Sem os cuidados adequados, a praticidade das transações on-line pode ser explorada por golpistas e criminosos, que utilizam técnicas sofisticadas para obter acesso não autorizado às contas, roubar informações pessoais ou cometer fraudes financeiras. Por isso, é fundamental seguir boas práticas de segurança para minimizar os riscos e garantir que suas transações sejam realizadas de forma segura.

Para se proteger e evitar prejuízos, adote precauções simples, como usar senhas fortes e únicas, ativar a autenticação de dois fatores e verificar a autenticidade dos aplicativos e sites que você utiliza. Manter seu dispositivo atualizado e monitorar suas contas regularmente também são passos importantes para garantir a segurança das suas transações financeiras.

USE SENHAS FORTES:

Mesmo com a biometria, o celular sempre exige uma senha ou padrão de desbloqueio. Se essa senha for fraca, um invasor pode facilmente quebrá-la e acessar seus dados.

Escolha uma senha longa e alfanumérica.

Evite padrões de desbloqueio simples.

Ative o bloqueio automático da tela com o menor intervalo de tempo disponível.

SENHA FORTE + BIOMETRIA NOS APLICATIVOS:

Aplicativos financeiros geralmente usam senha e biometria para controlar o acesso. No entanto, uma senha fraca pode comprometer a segurança da sua conta.

Crie uma senha forte para acesso via aplicativo.

Ative a biometria para facilitar o acesso.

Não repita senhas em diferentes aplicativos.

NÃO GRAVE A SENHA NOS APLICATIVOS:

Senhas armazenadas podem ser acessadas facilmente por criminosos.

Não salve senhas em blocos de notas, contatos ou navegadores.

Não envie senhas por mensagem ou e-mail.

Não tire fotos de senhas.

APENAS APLICATIVOS OFICIAIS:

Aplicativos falsos podem se disfarçar como versões oficiais e comprometer sua segurança.

Use apenas a loja oficial do sistema ou do fabricante.

Verifique o nome do aplicativo e do desenvolvedor antes de instalar.

MANTENHA OS APLICATIVOS ATUALIZADOS:

Vulnerabilidades podem ser exploradas por malware e outros ataques.

Instale atualizações regularmente para corrigir falhas de segurança.

Ative as atualizações automáticas.

Verifique as permissões dos aplicativos e remova aqueles desnecessários.

INSTITUIÇÕES NÃO ENTRAM EM CONTATO:

Instituições financeiras não solicitam informações pessoais por telefone, e-mail ou mensagem.

Desconfie de pedidos de informações pessoais.

Verifique a autenticidade da solicitação através de canais oficiais.

Nunca forneça dados pessoais em resposta a mensagens não solicitadas.

CARTÕES DE CRÉDITOS VIRTUAIS:

O cartão de crédito virtual pode ser gerado por um aplicativo e oferece segurança adicional.

Use o cartão virtual para pagamentos on-line.

Reduza o limite do cartão virtual.

Atualize os dados do cartão virtual regularmente.

OPEN FINANCE (COMPARTILHAMENTO DE INFORMAÇÕES)

Compartilhar dados financeiros com instituições não autorizadas pode comprometer sua privacidade.

Use aplicativos apenas das instituições participantes do *Open Finance*.

Verifique se a instituição financeira é regulamentada antes de compartilhar informações.

Monitore regularmente suas contas e dados financeiros para identificar atividades suspeitas.

CAPÍTULO 11

PROTEÇÃO PARA AS CRIANÇAS

No contexto da era digital contemporânea, as crianças estão mais conectadas do que em qualquer outro momento da história. A internet oferece uma vasta gama de oportunidades para aprendizado e socialização; no entanto, também expõe os jovens a riscos significativos, como roubo de identidade e a presença de predadores virtuais. Esses perigos podem comprometer a segurança e o bem-estar das crianças, caso não sejam devidamente gerenciados.

Para os pais e responsáveis, é imperativo compreender a importância da segurança cibernética a fim de proteger as crianças e adolescentes sob seus cuidados. Familiarizar-se com as ameaças presentes no ambiente on-line e entender como elas podem afetar a vida das crianças é o primeiro passo para assegurar uma navegação segura e saudável.

Este guia apresenta um conjunto de etapas essenciais para ajudá-lo a proteger as crianças no ambiente digital. Ao seguir essas recomendações, será possível resguardar informações pessoais e garantir que a experiência on-line das crianças seja mais segura e positiva.

SEUS FILHOS TÊM IDADE SUFICIENTE PARA O MUNDO DIGITAL?

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

Diversos estudos mostram os impactos negativos que o acesso à equipamentos eletrônicos na infância podem causar, em especial, o acesso ao aparelho celular. Recomendamos fortemente aos pais e educadores que não entreguem aparelhos de celular a crianças antes dos 14 anos e que adiem o acesso às redes sociais até os 16 anos. De acordo com o Movimento Desconecta, os celulares:

1. SÃO ALTAMENTE VICIANTES

Estudos indicam que a dependência do smartphone produz as mesmas respostas cerebrais que a dependência ao álcool, drogas e jogos. Os aparelhos e aplicativos são intencionalmente desenhados para isso.

2. REDUZEM O DESEMPENHO ACADÊMICO

O uso excessivo de telas diminui o desempenho em testes de QI, raciocínio e linguagem, bem como a capacidade cognitiva e de concentração.

3. PREJUDICAM O SONO

Tanto a qualidade, quanto o tempo de sono são afetados, prejudicando o bom desenvolvimento físico e mental de crianças e adolescentes

4. INTERFEREM NOS RELACIONAMENTOS

Os relacionamentos entre pais e filhos e entre os jovens são afetados pela distração e competição que o smartphone oferece. Desenvolver habilidades emocionais e sociais é fundamental!

5. AUMENTAM O RISCO DE ANSIEDADE E DEPRESSÃO

Crianças e adolescentes não têm maturidade neurológica para navegar nas redes sociais, com estimulação constante do cérebro e comparações irreais que causam o aumento dos níveis de cortisol.

6. COLOCAM SEU FILHO EM RISCO DE CYBER BULLYING

O bullying não está mais limitado ao playground ou ao vestiário. Há aumento de oportunidade e vulnerabilidade tanto para agressores quanto para agredidos.

7. EXPÕEM CRIANÇAS A CONTEÚDO SEXUAL

Além do acesso facilitado à pornografia, vários apps abrem as portas para predadores sexuais.

8. ALTERAM O CÉREBRO DAS CRIANÇAS

A longo prazo o córtex cerebral sofre alterações morfológicas prematuras importantes com o constante uso de telas.

Diante deste importante alerta, esclarecemos abaixo as precauções a serem tomadas para cada idade no controle e supervisão dos pais e educadores com relação ao uso de aparelho celular e outros equipamentos eletrônicos como tablets e televisão.

MENOR OU IGUAL A 5 ANOS DE IDADE:

As crianças ainda estão desenvolvendo uma compreensão do mundo, inclusive da internet, sendo fundamental que os pais supervisionem e restrinjam a atividade on-line. Por exemplo:

Manter os dispositivos ao alcance e à vista.

Configurar controles parentais.

Escolher conteúdo adequado à idade.

Nessa faixa etária, as crianças ainda não compreendem os riscos do comportamento on-line, portanto, esteja sempre atento e não as deixe com dispositivos eletrônicos sem a devida supervisão.

ALERTA: Idealmente, crianças nesta faixa de idade não deveriam utilizar equipamentos eletrônicos.

DE 6 A 10 ANOS DE IDADE:

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

As crianças começam a explorar a internet por conta própria, sendo fundamental que os pais apresentem a elas conceitos básicos de segurança cibernética, como:

Usar senhas fortes.

Não compartilhar informações pessoais.

Pensar antes de acessar um link.

Os pais devem orientar seus filhos sobre quais sites, jogos e aplicativos são seguros e apropriados para a idade deles. É fundamental que estejam cientes da atividade on-line dos filhos e, caso encontrem algo desconfortável, incentivem-nos a relatar. Além disso, evitem deixá-los sem a devida supervisão ao usar dispositivos eletrônicos.

ALERTA: Idealmente, crianças nesta faixa de idade não deveriam utilizar equipamentos eletrônicos.

DE 11 A 15 ANOS DE IDADE:

À medida que os filhos entram na adolescência, podem começar a usar mídias sociais e jogos on-line com mais frequência. É fundamental que os pais apresentem conceitos mais avançados de segurança cibernética, como:

Autenticação multifatorial (MFA).

Como evitar o bullying on-line.

Desconfiar de tudo e de todos.

Os pais devem ensinar seus filhos sobre a importância das configurações de privacidade e garantir que eles estejam cientes dos possíveis impactos do compartilhamento de informações pessoais on-line. Ajude seus filhos a usarem a tecnologia de forma segura e monitore suas atividades on-line.

ALERTA: Idealmente, crianças nesta faixa de idade deveriam utilizar equipamentos eletrônicos somente com supervisão direta.

16 ANOS DE IDADE OU MAIS:

INCC
INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

Os adolescentes têm mais liberdade e independência on-line, o que os torna mais vulneráveis a ameaças, como:

Cyberbullying.

Golpes.

Roubo de identidade.

Mostre a seus filhos adolescentes como se manter seguros e identificar atividades suspeitas on-line. É importante ter uma comunicação aberta e honesta com eles, incentivando-os a compartilhar suas atividades, enquanto respeita a privacidade deles. Apoie-os na tomada de escolhas responsáveis, especialmente ao jogar e usar mídias sociais. Certifique-se de que estejam cientes dos possíveis impactos de suas ações on-line.

DICAS EXTRAS BULLYING TRADICIONAL VS. *CYBERBULLYING*

ASPECTO	BULLYING TRADICIONAL	CYBERBULLYING
ALCANCE	Geralmente limitado ao ambiente escolar ou local.	Pode ocorrer a qualquer hora e lugar.
PERMANÊNCIA	Geralmente temporário.	Conteúdo pode permanecer on-line indefinidamente.
ANONIMATO	Agressor geralmente conhecido.	Agressor pode permanecer anônimo.

DESATIVAR SEVIÇOS DE GEOLOCALIZAÇÃO

A geolocalização pode ajudar a manter o controle de seus filhos; no entanto, alguns aplicativos podem usar ou vender dados de localização para fins comerciais. Para garantir a segurança, os pais devem desativar a geolocalização para cada aplicativo nas configurações do dispositivo e considerar excluir aplicativos quando isso não for possível.

É importante que os pais, junto com os filhos, verifiquem os aplicativos que desejam instalar, descubram quais dados são coletados e ativem as configurações de segurança e privacidade relevantes. Sempre explique a importância de ter cuidado com as permissões concedidas aos aplicativos.

A geolocalização pode ajudá-lo a manter o controle de seus filhos; no entanto, alguns aplicativos podem usar ou vender dados de localização para fins comerciais. Para garantir a segurança, os pais devem desativar a geolocalização para cada aplicativo nas configurações do dispositivo e considerar excluir aplicativos quando isso não for possível.

COMPARTILHAMENTO DE DISPOSITIVOS FAMILIARES

Os pais às vezes permitem que seus filhos usem seus *smartphones* ou tablets; porém, é fundamental considerar quais dados, aplicativos e sites estão instalados. Permitir que uma criança use seu dispositivo sem medidas de segurança pode colocar a família em risco. Limpe o histórico do navegador com frequência para limitar o acesso às suas contas e dados privados. Não compartilhe suas senhas e *PINs* com seus filhos; isso garante que eles precisem perguntar antes de usar seu dispositivo ou acessar a internet.

JOGOS ON-LINE

Os jogos on-line são populares entre as crianças, mas é importante que os pais estejam cientes dos riscos de segurança cibernética associados a eles. Ao jogar, as crianças podem interagir com estranhos que têm intenções maliciosas. Ensine seus filhos a não compartilharem detalhes pessoais com quem não conhecem, pois os cibercriminosos podem se passar por amigos. Explique que eles devem estar atentos a golpes de *phishing*, que podem incluir ofertas de atualizações gratuitas, moedas do jogo ou itens raros de personagens. Antes de baixar qualquer jogo, os pais e filhos devem verificar a fonte. Ativar controles parentais em dispositivos e aplicativos de jogos pode ajudar no monitoramento.

MÍDIA SOCIAL

Se seus filhos usam redes sociais, eles podem ter "amigos" ou "seguidores" que não conheceram na vida real. Além disso, podem seguir suas celebridades favoritas ou sites oficiais de fãs. Muitos sites oficiais de notícias sobre celebridades e entretenimento são seguros, mas é fácil para as pessoas fingirem ser outra pessoa na internet. É importante ajudar seus filhos a navegarem no mundo digital para garantir sua segurança on-line. A orientação é a melhor prevenção.

DICAS EXTRAS PARA JOGOS ON-LINE E MÍDIA SOCIAL

Aqui estão algumas dicas adicionais de segurança para seus filhos quando estiverem nas mídias sociais e jogando:

Use software legítimo: Sempre utilize aplicativos e jogos de empresas oficiais e confiáveis, incluindo lojas físicas ou lojas de aplicativos.

Evite salvar detalhes de pagamento: Sempre que possível, não salve detalhes de pagamento em suas contas. Alguns dispositivos têm configurações que solicitam uma senha ao fazer o download de um aplicativo, e você também pode configurar o aplicativo para solicitar sua senha após um período de inatividade.

Seja cauteloso com estranhos: Ensine seus filhos a verificarem se conhecem a pessoa on-line. Se não souberem, devem pedir ajuda e na dúvida, não devem interagir.

Desconfie de mensagens não solicitadas: Se alguém que seu filho não conhece entrar em contato, ensine-o a ignorar e a contar para você.

MONITORE A PRESENÇA ON-LINE DE SEUS FILHOS

Diga a seus filhos para não compartilharem informações pessoais ou confidenciais nas redes sociais, como informações pessoais, endereço residencial, a data de nascimento ou fotos. Verifique as configurações de privacidade da conta de seu filho para saber quem pode ver seus detalhes. Esteja ciente das restrições de idade nas redes sociais e certifique-se de que seus filhos entendam as diretrizes.

DESCONFIE DE SOLICITAÇÕES SOBRE INFORMAÇÕES PESSOAIS NÃO SOLICITADAS

Ensine seus filhos a estabelecerem limites sobre o que compartilham on-line. Incentive-os a manter perfis privados, não compartilhando números de telefone, endereço residencial ou escolar, data de nascimento ou fotos. Isso inclui evitar compartilhar qualquer coisa que possa revelar esses detalhes, como um uniforme escolar em uma foto.

Os golpistas costumam fazer com que as pessoas forneçam informações financeiras ou abram arquivos. Diga a seus filhos para bloquearem qualquer perfil incomum ou mal-intencionado, utilizando a opção "bloquear" no perfil do usuário.

VERIFIQUE O URL DOS SITES PARA GARANTIR QUE SEJAM LEGÍTIMOS

Ao acessar um site, certifique-se de que o endereço (URL) seja verdadeiro. Os golpistas podem criar sites falsos que se parecem com os verdadeiros, induzindo você e seus filhos a fornecerem informações pessoais. Verifique se o nome do domínio e a ortografia estão corretos; isso pode ser difícil de detectar, pois pode haver apenas uma letra diferente. Ao fazer pagamentos on-line, a URL deve começar com "https" (o "s" significa seguro) e ter o nome da empresa no domínio.

Não abra links nem utilize detalhes de contato enviados a você. Em caso de dúvida, entre em contato com a empresa por meio das informações disponíveis em seu site oficial.

DESCONFIE DE OFERTAS QUE PAREÇAM BOAS DEMAIS PARA SEREM VERDADEIRAS

Os golpistas podem oferecer algo tentador, como férias gratuitas ou dinheiro. Lembre-se de que, se parecer bom demais para ser verdade, provavelmente é. Diga a seus filhos para consultá-lo antes de fornecer dados pessoais ou dinheiro. Nem todos on-line são quem dizem ser; incentive seus filhos a verificarem se conhecem a pessoa. Ensine-os a não acessar links ou fazer download de arquivos de pessoas desconhecidas.

INCENTIVEM SEUS FILHOS A PERGUNTAREM

Seus filhos podem não ter certeza se algo é um golpe ou se alguém está pedindo informações sobre ele/ela ou sobre a família. Explique que devem pedir ajuda para determinar se a solicitação é real ou falsa. Se você ainda não tiver certeza, é melhor ignorar a solicitação.

VAZAMENTO DE NUDES E EXPOSIÇÃO DE INTIMIDADE

Explique e ensine que o compartilhamento de imagens íntimas é muito perigoso e pode ter consequências tanto para seus filhos quanto para a família. Jamais compartilhe imagens de terceiros sem autorização expressa, respeitando sempre a privacidade alheia. O compartilhamento não autorizado de imagens íntimas é crime, conforme a Lei nº 13.718/2018, e os infratores podem enfrentar processos judiciais e penas de prisão.

Caso a criança ou adolescente seja vítima, ensine-os a buscar apoio emocional junto a vocês e/ou profissionais especializados, e a denunciar imediatamente às autoridades competentes. Lembre-se sempre de informar seus filhos: uma vez na internet, controlar sua distribuição torna-se extremamente difícil.

Lista de Verificação de Segurança Cibernética

1. **Configure o Controle dos Pais nos Dispositivos**

   Limite o acesso a conteúdo inadequado e restrinja sites, aplicativos e serviços.

2. **Converse com Seus Filhos sobre Segurança On-line**

   Explique os perigos como predadores, *cyberbullying*, golpes e roubo de identidade. Incentive a comunicação e a conversa sobre dúvidas e preocupações.

3. **Use Senhas Fortes e Exclusivas**

   Certifique-se de que seus filhos criem senhas robustas, como frases de acesso. Considere um gerenciador de senhas seguro.

4. **Use a Autenticação Multifator (MFA)**

   Ative a MFA em todos os dispositivos e serviços que a suportam para uma camada extra de segurança.

5. Mantenha o Software Atualizado

Atualize frequentemente software e sistemas operacionais para corrigir vulnerabilidades de segurança.

6. Use Software Antivírus

Instale e mantenha um software antivírus em todos os dispositivos para proteção contra *malware* e vírus.

7. Faça Backup de Dados Importantes

Realize backups regulares de fotos, documentos e vídeos, armazenando-os em um disco rígido externo ou na nuvem.

8. Desconfie Sempre

Ensine seus filhos a serem cautelosos com e-mails, mensagens de texto ou chamadas não solicitadas que peçam informações pessoais.

9. Monitore as Atividades On-line de Seus Filhos

Fique atento aos sites que visitam e aos aplicativos que usam.

10. Ensine Seus Filhos a Relatar Incidentes

Oriente-os a denunciar *cyberbullying* e a falar com você ou um adulto de confiança sobre assédio ou comportamentos inadequados.

A SEGURANÇA CIBERNÉTICA COMEÇA COM CADA UM DE NÓS, E JUNTOS PODEMOS CONSTRUIR UM AMBIENTE DIGITAL MAIS SEGURO PARA TODOS.

MANTENHA-SE SEGURO!

@inccbrasil

www incc.org.br

INCC

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

@inccbrasil

www incc.org.br