PHISHX

Dicas de segurança cibernética para profissionais da saúde

Segurança na Saúde

Para médicos, enfermeiros, e atendentes, a confiança dos pacientes é um pilar fundamental da prática da saúde. Esta confiança se estende além do cuidado clínico para incluir a segurança dos dados pessoais dos pacientes.

Dessa forma, uma violação pode não apenas erodir a confiança do paciente, mas também expor informações sensíveis e colocar em risco a integridade da instituição de saúde. Reconhecendo a importância de fortalecer a segurança cibernética, esta cartilha é dedicada à profissionais da saúde, oferecendo orientações práticas para proteger os dados dos seus pacientes contra ameaças digitais. Juntos, podemos construir um ambiente mais seguro para nossos pacientes e para o nosso trabalho.

Compreendendo os Riscos Cibernéticos

Para médicos, enfermeiros, e atendentes que trabalham diariamente com dados de pacientes, compreender os riscos cibernéticos é o primeiro passo para construir uma defesa eficaz. Os dados de saúde são extremamente valiosos para criminosos digitais, tornando o setor de saúde um alvo frequente de ataques.

O impacto desses riscos vai além das consequências imediatas de um ataque específico. Eles podem afetar a integridade do atendimento ao paciente, levar a perdas financeiras significativas e danificar a reputação de uma instituição de saúde a longo prazo. Por isso, é importante conhecer as principais ameaças e saber como elas podem ser um risco para os pacientes e para os negócios.

Violações de Dados

Violações de dados ocorrem quando informações confidenciais são expostas, seja por ataques externos, como hacking, ou falhas internas, como um funcionário compartilhando acidentalmente dados sensíveis.

Para um paciente, isso pode significar a exposição de seus históricos médicos, informações de seguro e outros dados pessoais. Para a instituição, as consequências vão desde multas pesadas até a perda de confiança do paciente.

Ransomware

Ransomware é um tipo de malware que criptografa os arquivos do sistema, exigindo um resgate para a liberação. Hospitais e clínicas são alvos particularmente atrativos para esses ataques devido à necessidade crítica de acesso contínuo aos dados dos pacientes. Um ataque de ransomware pode paralisar completamente as operações, comprometendo o atendimento ao paciente.

Phishing

Ataques de phishing frequentemente visam profissionais da saúde para ganhar acesso a sistemas internos. Esses ataques podem assumir a forma de e-mails ou mensagens que parecem legítimos, enganando os funcionários para que revelem senhas ou instalem software malicioso.

Ameaças Internas

Não são apenas os atacantes externos que representam um risco, os funcionários também podem, acidentalmente ou intencionalmente, causar violações de dados. Isso pode ser desde um atendente perdendo um laptop com informações de pacientes até um médico acessando dados de saúde sem necessidade.

Dicas Práticas de Segurança Cibernética

Na linha de frente do atendimento ao paciente, médicos, enfermeiros e atendentes desempenham um papel crucial na proteção contra ameaças cibernéticas. Implementar práticas de segurança robustas não só protege as informações dos pacientes, mas também preserva a integridade do sistema de saúde.

Aprenda sobre phishing e engenharia social

Participe de treinamentos sobre segurança cibernética oferecidos pela instituição para reconhecer e responder a tentativas de phishing e outros tipos de engenharia social. Antes de fornecer qualquer informação ou clicar em links em e-mails, verifique a autenticidade da solicitação, especialmente se pedir informações sensíveis.

Utilize senhas fortes e a autenticação em dois fatores

Utilize senhas longas, complexas e únicas para cada sistema ou aplicativo. Considere o uso de frases de senha, que são longas, mas fáceis de lembrar. Mude suas senhas regularmente e nunca as reutilize entre diferentes contas ou serviços. Sempre que possível, ative a autenticação de dois fatores para adicionar uma camada extra de segurança.

Proteja seus dispositivos

Garanta que seu telefone, tablet ou laptop esteja sempre bloqueado com senha, PIN, ou biometria quando não estiver em uso. Lembre-se de manter o sistema operacional e os aplicativos atualizados para proteger contra vulnerabilidades conhecidas.

Procure acessar o mínimo necessário de dados

Acesse apenas as informações dos pacientes que são estritamente necessárias para o tratamento ou diagnóstico. Isso limita a exposição de dados sensíveis. Além disso, tenha cautela ao compartilhar informações dos pacientes, mesmo dentro da equipe de saúde. Certifique-se de que a pessoa que recebe os dados realmente precisa deles para fins de tratamento.
Implementando essas medidas, médicos e outros profissionais de saúde podem desempenhar um papel crucial na prevenção de vazamentos de dados, protegendo assim a privacidade e a segurança dos pacientes. Estas ações, quando integradas como parte da rotina diária, fortalecem a cultura de segurança cibernética dentro das organizações de saúde