ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DEPUTADO ROBERTO MESQUITA

EVELLYN CLEYCIANE SOUSA LIMA

A NOVA REALIDADE DO TRABALHO REMOTO:
RISCOS E BOAS PRÁTICAS DE CIBERSEGURANÇA PARA EMPRESAS DISTRIBUÍDAS

GENERAL SAMPAIO- CEARÁ
2024

INTRODUÇÃO:

A pandemia de COVID-19 acelerou a adoção do trabalho remoto em todo o mundo, transformando a maneira como as empresas operam. Embora essa mudança tenha trazido inúmeros benefícios, como maior flexibilidade e redução de custos, também introduziu novos desafios, especialmente em termos de cibersegurança. Empresas distribuídas, com funcionários trabalhando de diferentes locais, precisam estar atentas aos riscos cibernéticos e adotar práticas eficazes para proteger seus dados e sistemas.

RISCOS DE CIBERSEGURANÇA NO TRABALHO REMOTO

Acesso não autorizado: Redes Wi-Fi domésticas podem ser menos seguras do que as redes corporativas, aumentando o risco de invasões.
Phishing e engenharia social: A comunicação digital intensificada torna os funcionários mais suscetíveis a ataques de phishing.
Uso de dispositivos pessoais: Dispositivos pessoais podem não ter as mesmas proteções que os dispositivos corporativos, expondo dados sensíveis a malware.
Falta de atualizações: Dispositivos sem atualizações regulares de segurança são mais vulneráveis a ataques.

BOAS PRÁTICAS DE CIBERSEGURANÇA

Uso de VPN: Implementar uma Rede Privada Virtual (VPN) para garantir que todas as comunicações sejam criptografadas e seguras.
Autenticação de dois fatores (2FA): Adotar a autenticação de dois fatores para adicionar uma camada extra de segurança no acesso aos sistemas corporativos .
Treinamento de funcionários: Capacitar os colaboradores sobre as melhores práticas de cibersegurança, incluindo como identificar e evitar ataques de phishing.
Políticas de segurança claras: Estabelecer políticas de segurança cibernética que definam claramente as responsabilidades e procedimentos para proteger os dados da empresa.
Atualizações regulares: Garantir que todos os dispositivos usados para trabalho remoto estejam sempre atualizados com os patches de segurança mais recentes.

CONCLUSÃO

A transição para o trabalho remoto trouxe consigo uma série de desafios de cibersegurança que não podem ser ignorados. Empresas distribuídas precisam adotar uma abordagem proativa para proteger seus dados e sistemas, implementando políticas claras, treinamentos regulares e tecnologias de segurança robustas. Ao seguir essas boas práticas, é possível minimizar os riscos e garantir que o trabalho remoto seja seguro e eficiente para todos os envolvidos.