Trabalho remoto: O que você deve saber para trabalhar de forma segura?

por Saulo Meneghini, CEO e Founder Pinpoint

Índice

A pandemia fez com que negócios adotassem o modo de trabalho remoto para a maioria das funções

Pandemia e o novo modo de trabalho

Antes	Agora
Acesso à recursos/ aplicações era extremamente limitado e protegidos	Todos os recursos / aplicações devem estar disponíveis
Investimentos de TI eram focados para a rede corporativa	Sem tempo para um planejamento de segurança adequado
Serviços financeiros consumiam em média 10% do orçamento de TI em segurança cibernética Isso é aproximadamente 0,2% a 0,9% da receita da empresa ou US$ 1.300 a US$3.000 por funcionário em tempo integral*	Funções que tradicionalmente eram desempenhadas no escritório (Exemplo: CallCenter) se adequaram ao trabalho remoto
	Redes domésticas são negligenciadas ou não estão preparadas para tal função
	Investimentos em segurança cibernética ainda não cobrem redes domésticas

*Fonte: Deloitte

Pandemia e o novo modo de trabalho

Antes	Agora
Acesso à recursos/ aplicações era extremamente limitado e protegidos	Todos os recursos / aplicações devem estar disponíveis
Investimentos de TI eram focados para a rede corporativa	Sem tempo para um planejamento de segurança adequado
Serviços financeiros consumiam em média 10% do orçamento de TI em segurança cibernética	Funções que tradicionalmente eram desempenhadas no escritório (Exemplo: CallCenter) se adequaram ao trabalho remoto
Isso é aproximadamente 0,2% a 0,9% da receita da empresa ou US$ 1.300 a US$3.000 por funcionário em tempo integral*	Redes domésticas são negligenciadas ou não estão preparadas para tal função
	Investimentos em segurança cibernética ainda não cobrem redes domésticas

*Fonte: Deloitte

Pandemia e o novo modo de trabalho

Antes	Agora
Acesso à recursos/ aplicações era extremamente limitado e protegidos	Todos os recursos / aplicações devem estar disponíveis
Investimentos de TI eram focados para a rede corporativa	Sem tempo para um planejamento de segurança adequado
Serviços financeiros consumiam em média 10% do orçamento de TI em segurança cibernética Isso é aproximadamente 0,2% a 0,9% da receita da empresa ou US$ 1.300 a US$3.000 por funcionário em tempo integral*	Funções que tradicionalmente eram desempenhadas no escritório (Exemplo: CallCenter) se adequaram ao trabalho remoto
	Redes domésticas são negligenciadas ou não estão preparadas para tal função
	Investimentos em segurança cibernética ainda não cobrem redes domésticas

*Fonte: Deloitte

Trabalho Remoto é uma tendência

74%

das organizações dizem que 50-100% dos colaboradores trabalham em casa

86%

Dizem que continuarão com esse modo de trabalho

*Fonte: Databasix UK

Rede corporativa X doméstica

A rede doméstica se torna parte da corporativa a partir do momento em que se conecta à ela

Embora organizações estejam investindo pesadamente em redes corporativas, redes domésticas não estão sob seu controle

Rede corporativa X doméstica

Hackers estão explorando ativamente fraquezas das redes domésticas para atacar

O trabalho remoto se tornou a porta de entrada para as redes corporativas

Cibercriminosos estão adaptando suas técnicas de ataque

O assunto “COVID-19” ou “Pandemia” foi classificado como a maior ameaça de segurança cibernética de todos os tempos.
Não é apenas o gerenciamento de segurança dentro das organizações que está deficiente, mas também dos colaboradores

2 equívocos comuns sobre segurança de rede

"A rede doméstica é muito pequena para correr risco de um ciber ataque"

"Os equipamentos da empresa são seguros o suficiente"

(Fonte: CISA - US Gov)

A verdade

A maioria dos ataques não são de natureza pessoal e podem ocorrer em qualquer tipo de rede - grande ou pequena, doméstica ou comercial

Se a rede se conecta à Internet, se torna consequentemente vulnerável e suscetível a ameaças externas

Dados relacionados ao trabalho remoto e ataques cibernéticos após a pandemia

20% das organizações tiveram quebras de segurança por causa de trabalhadores remotos

630% de aumento nos ataques à redes baseadas em cloud

600% de crescimento médio em disparos de phishing e-mails

24% das organizações tiveram despesas inesperadas para resolver uma violação de segurança ou ataque de malware após a mudança para o trabalho remoto

Fontes: Databasix, Varonis, Barracuda, Google, IBM, Deloitte

Dados relacionados ao trabalho remoto e ataques cibernéticos após a pandemia

26%

dos funcionários relataram se sentir tentados a manter cópias locais de dados da empresas onde trabalham

US$137 mil

aumento médio no custo de uma violação de dados com o modo trabalho remoto

44%

das organizações não forneceram treinamento de segurança cibernética às equipes sobre as ameaças de trabalhar em casa

81%

dos profissionais de segurança cibernética relataram que suas funções mudaram durante a pandemia

Fontes: Databasix, Varonis, Barracuda, Google, IBM, Deloitte

Dados relacionados ao trabalho remoto e ataques cibernéticos após a pandemia

36 bi
de dados foram expostos por violações no primeiro semestre de 2021

86%
foram motivadas por ganhos financeiros

10%
por espionagem corporativa

32%
dos ataques incluíram hacking

17%
continham malwares

35%
phishing

Fontes: Databasix, Varonis, Barracuda, Google, IBM, Deloitte

Dados relacionados ao trabalho remoto e ataques cibernéticos após a pandemia

500 mil

de contas do Zoom foram comprometidas e vendidas em um fórum na dark web em abril de 2020

100 milhões

De e-mails contendo phishing são bloqueados pelo Gmail todos os dias

Por que redes domésticas são tão vulneráveis?

Por que redes domésticas são tão vulneráveis

- A maioria das redes domésticas são padrão do fabricante, com segurança básico ou muitas vezes nenhuma
- 86% dos usuários contam com o roteador Wi-Fi padrão básico fornecido pelo provedor de internet
- Os populares dispositivos IoT são muito simples, vulneráveis e não possuem recursos de segurança
- A maioria dos dispositivos de rede doméstica nunca são atualizados

Por que redes domésticas são tão vulneráveis

Não há controle, auditorias, varreduras, avaliações ou processos para garantir um nível mínimo de segurança

Qualquer pessoa e dispositivo acessam a rede sem análise prévia de ameaças

Usuários domésticos não estão cientes dos riscos e tendem a ser mais brandos em relação à segurança

Todos têm níveis de acesso como administrador para a maioria dos dispositivos e recursos

Dicas de segurança em redes domésticas para usuários

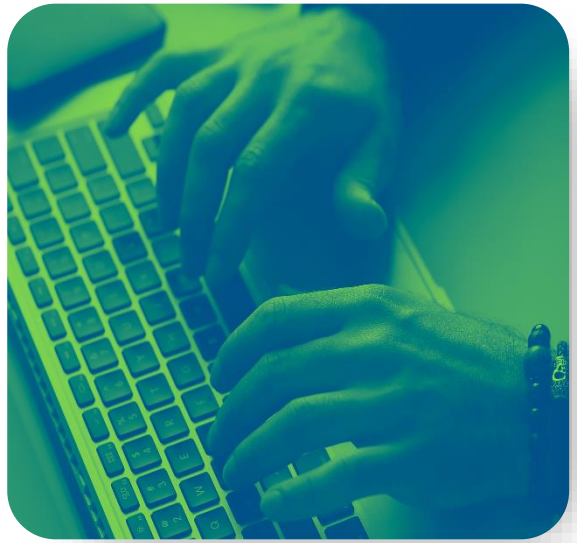
Dicas de segurança em redes domésticas para usuários

Ter uma rede doméstica segura protege não só as organizações, mas também suas informações e dados

Muito do que você aprende com os treinamentos de segurança podem ser replicados em casa

Esteja ciente da engenharia social

A tecnologia por si só não garante proteção. Você é a melhor defesa



Mecanismos mais comuns usados na engenharia social

Senso de urgência
Por meio de intimidação, crise ou um prazo importante

Pressão
Para ignorar políticas e procedimentos de segurança

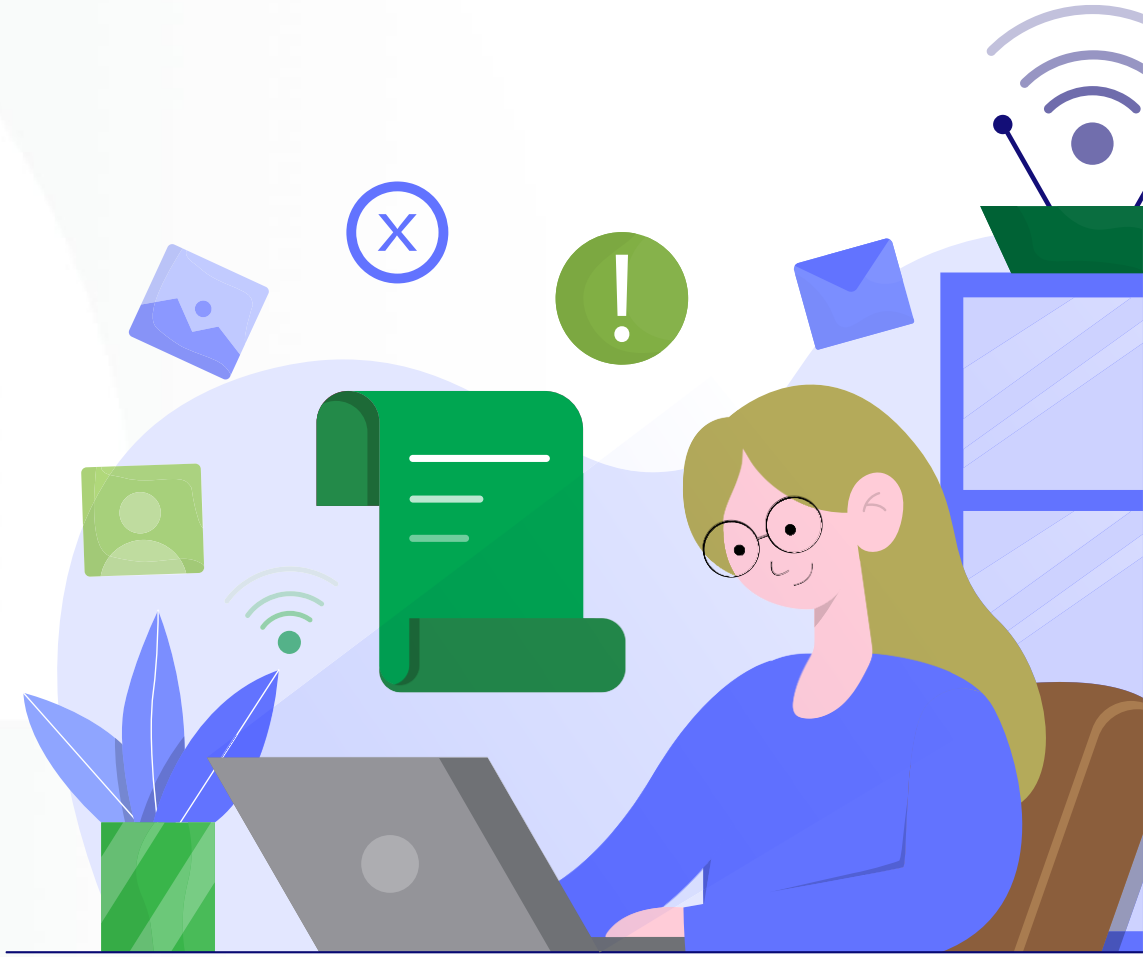
Falsificação de identidade
Envio de mensagens em que a assinatura, tom de voz ou a redação não parecem com eles

Uma oferta irrecusável
Com mensagens e valores fora do comum para chamar a atenção

Dicas de segurança em redes domésticas para usuários

Invista em uma rede WI-FI moderna e com recursos de segurança, como:

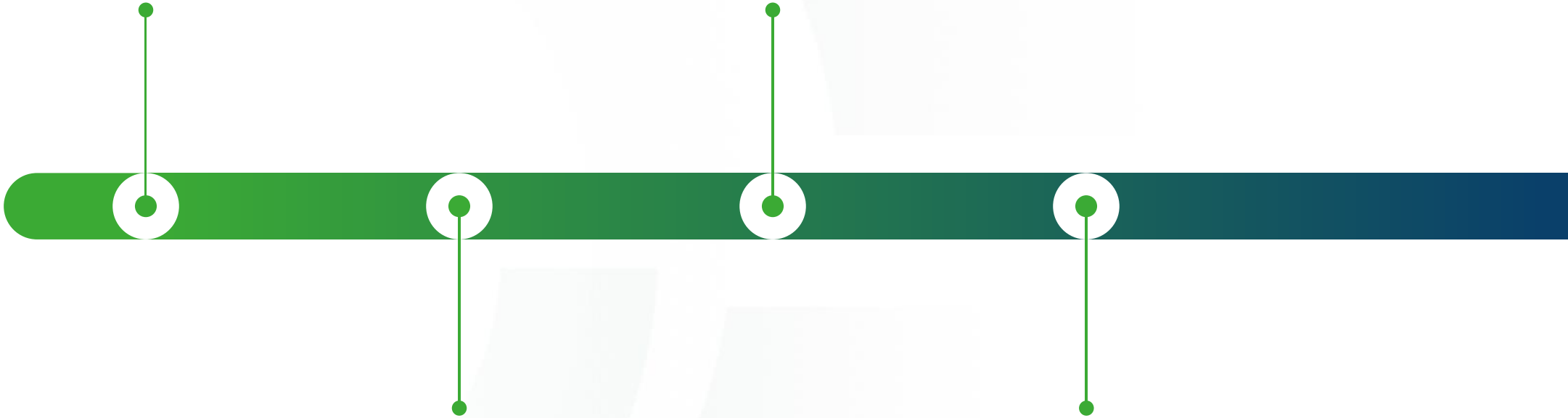
- Segregação de "Redes de convidados" e /ou "Redes de quarentena"
- Mecanismos de lista branca /negra
- Filtragem de conteúdo
- Controle de acessos (Parental Controls)
- Alertas de quebra de segurança



Dicas de segurança em redes domésticas para usuários

Tudo o que estiver conectado à rede doméstica é um potencial vetor de ataque

Conheça todos os seus dispositivos e mantenha-os atualizados com a versão /firmware mais recente. Especialmente IoTs



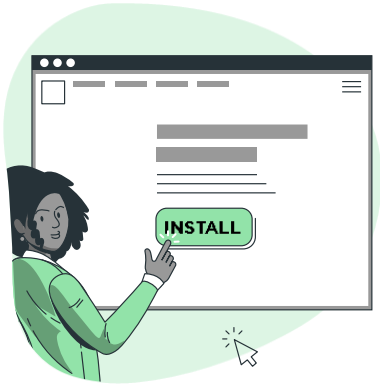
Antes de comprar qualquer dispositivo IoT, verifique os recursos de segurança oferecidos pelo fornecedor e também se é EOL!

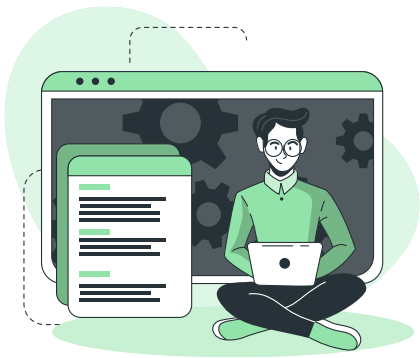
Alterar as senhas de administrador padrão

Dicas de segurança em redes domésticas para usuários

Antivírus instalado em todos os dispositivos

A maioria dos fornecedores oferece "Pacotes familiares" que podem cobrir todas as suas necessidades por um preço acessível





Contas de administrador

Limite os acessos, criando usuários nomeados e exclusivos para cada familiar

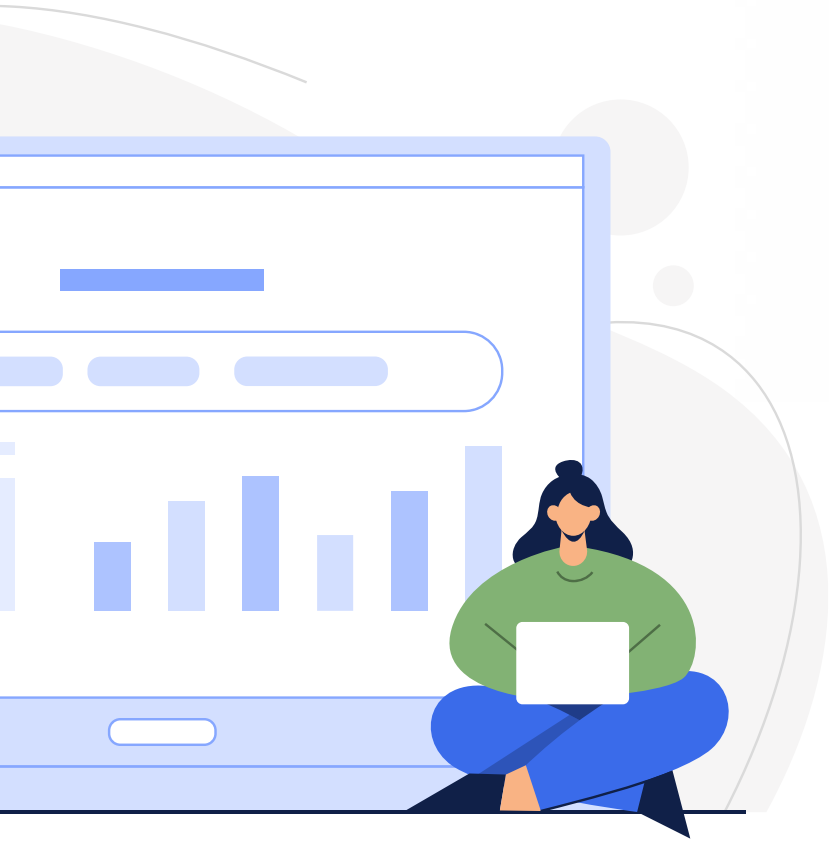
Senhas

Use um aplicativo pra gerenciá-las (ex: LastPass, 1Password), nunca salve em texto simples ou planilhas do Excel!

Autenticação multifator

Ative quando possível (Amazon, WhatsApp, Facebook, etc. já suportam)

Dicas de segurança em redes domésticas para usuários



Dispositivos corporativos são recursos CORPORATIVOS. Não compartilhe em nenhuma circunstância e não use para fins pessoais

Evite WI-FIs públicos e limite tempo de acesso aos recursos que a TI sinaliza como seguros para qualquer lugar - Exemplo: Office 365

Lembre-se de usar o navegador nos modos privado/ Incógnito e limpar o cache/ histórico do navegador quando terminar

Em nenhuma circunstância instale VPN em clientes de dispositivos não corporativos

Iniciativas de TI para garantir um trabalho remoto seguro

#1

Educar a equipe no gerenciamento de dados confidenciais em casa

#2

Fornecer todos os recursos possíveis e necessários para um trabalho remoto seguro

#3

Monitorar todos os dispositivos usados para identificar e solucionar rapidamente erros e contratempos

Iniciativas de TI para garantir um trabalho remoto seguro

#4 Adote soluções baseadas em IA para análise do comportamento do usuário e/ou entidade do usuário

#5 Validação da eficácia de segurança em prestadores de serviços, fornecedores e parceiros, garantindo que não haja fraquezas na cadeia de abastecimento

#6 Avaliar a capacidade de lidar com um ataque cibernético de forma rápida e eficiente, bem como os níveis de recuperação para garantir que as infraestruturas de TI voltem a funcionar o mais rápido possível

Tem um desafio?

Fale com a gente.

(11) 3900.1391
comercial@pinpoint.com.br
pinpoint.com.br

pinpoint
keep IT on