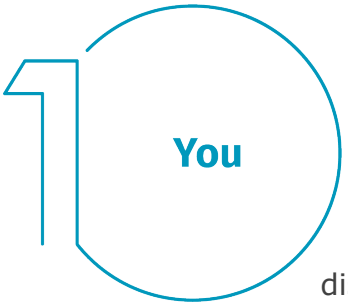
SANS SECURITY AWARENESS

5 passos para trabalhar em casa com segurança

Sabemos que trabalhar de casa pode ser algo novo para alguns de vocês, talvez até desnorteante enquanto nos ajustamos a esse novo ambiente. Um dos nossos objetivos é permitir que você trabalhe de casa com a maior segurança possível. Abaixo há cinco medidas simples para trabalhar com segurança. A melhor parte é que todas essas medidas não só ajudam a proteger seu trabalho, como também deixarão você e sua família mais protegidos, em um lar ciberneticamente seguro.



Você: Antes de mais nada, é importante saber que a tecnologia por si só não é capaz de protegê-lo totalmente. Você é a melhor defesa. Os atacantes já aprenderam que a melhor forma de conseguir o que querem é tendo você como alvo, em vez de seu computador ou outros dispositivos. Se quiserem sua senha, seus dados de trabalho ou controle do seu computador, eles tentarão enganar você e induzi-lo a dar isso a eles, muitas vezes criando um senso de urgência. Por exemplo, eles podem telefonar para você fingindo ser o suporte técnico da Microsoft e alegar que seu computador está infectado. Ou podem enviar um e-mail avisando que não foi possível entregar uma encomenda, enganando você e fazendo com que clique em um link malicioso. Os indicadores comuns de um ataque de engenharia social incluem:

- Alguém criando um enorme senso de urgência, muitas vezes através do medo, da intimidação, de uma crise ou de um prazo importante. Atacantes cibernéticos são bons em criar mensagens convincentes que parecem vir de organizações confiáveis, como bancos, o governo ou organizações internacionais.
- Pressão para que você ignore políticas ou procedimentos de segurança, ou uma oferta boa demais para ser verdade (não, você não ganhou na loteria!)
- Uma mensagem de um amigo ou colega de trabalho com uma assinatura, tom ou palavras que não parecem ser dele.

No fim, a melhor defesa contra esses ataques é você mesmo.

Rede Doméstica: Quase toda rede doméstica inclui uma rede sem fio (também chamada de Wi-Fi). É ela que permite que todos os seus dispositivos se conectem com a internet. A maioria das redes domésticas sem fio é controlada pelo roteador de internet ou um ponto de acesso sem fio dedicado, separado. Ambos funcionam da mesma maneira: transmitindo sinais sem fio que os dispositivos domésticos usam para se conectar. Isso significa que proteger sua rede sem fio é parte fundamental de proteger sua casa. Para isso, nós recomendamos as seguintes medidas:

- Altere a senha de administrador padrão do dispositivo que controla sua rede sem fio. A conta de administrador é o que permite alterar as configurações da sua rede sem fio.
- Certifique-se que apenas pessoas da sua confiança possam se conectar à sua rede sem fio. Para isso, habilite a segurança forte. Assim, as pessoas só conseguem se conectar à sua rede sem fio com uma senha. Além disso, depois de conectadas, suas atividades online permanecem criptografadas.
- Certifique-se de usar uma senha forte e diferente da senha de administrador para as pessoas se conectarem à sua rede sem fio. Não se esqueça de que só é necessário inserir a senha uma vez para cada dispositivo, pois eles armazenam e lembram a senha.

Não sabe como seguir esses passos? Peça ajuda ao seu provedor de internet, verifique o site deles, confira a documentação que veio com o ponto de acesso sem fio, ou consulte o site do fornecedor.

Senhas: Quando um site pedir para você criar uma senha, crie uma senha forte. Quanto mais caracteres ela tiver, melhor. Usar uma frase secreta é uma das formas mais simples de garantir uma senha forte. Uma frase secreta não passa de uma senha composta por várias palavras, como "*abelha mel uísque*". Usar uma frase secreta única significa criar diferentes frases para cada dispositivo ou conta online. Assim, se uma frase secreta for comprometida, todos os seus outros dispositivos e contas estarão seguros. Não consegue se lembrar de todas as frases secretas?

Use um gerenciador de senhas, um programa especializado que armazena todas as suas frases secretas com segurança em um formato criptografado (e também

inclui vários outros recursos excelentes!). Por fim, sempre que possível, habilite a verificação em duas etapas (também chamada de autenticação de fator duplo ou multifator). Além de usar sua senha, esse recurso adiciona uma segunda etapa, como um código enviado para o seu smartphone ou gerado por um aplicativo. A verificação em duas etapas é provavelmente a medida mais importante que você pode adotar para proteger suas contas online, e é muito mais simples do que talvez você esteja pensando.

Atualizações: Certifique-se de que todos os seus computadores, dispositivos móveis, programas e aplicativos estejam com a versão mais recente do software. Atacantes cibernéticos estão sempre em busca de novas vulnerabilidades nos softwares dos seus dispositivos. Quando descobrem vulnerabilidades, eles usam programas especiais para se aproveitar disso e invadir os seus dispositivos. Enquanto isso, as empresas que criaram os softwares nesses dispositivos trabalham duro para consertá-los, lançando atualizações. Assegurando que os seus computadores e dispositivos móveis instalem essas atualizações prontamente, você dificulta bastante o trabalho dos invasores. Para se manter atualizado, simplesmente habilite as atualizações automáticas sempre que possível. Essa regra se aplica a quase toda tecnologia conectada a uma rede, incluindo não só seus dispositivos de trabalho, mas também outros aparelhos que se conectam com a internet, como TVs, monitores de bebê, câmeras de segurança, roteadores, videogames, e até mesmo seu carro.

Crianças e convidados: Algo que provavelmente não é uma preocupação no escritório são crianças, convidados ou outros membros da família querendo usar seu laptop ou outros dispositivos de trabalho. Certifique-se que sua família e seus amigos entendam que não podem usar seus dispositivos de trabalho. Sem querer, eles podem acabar apagando ou modificando informações, ou até pior, infectando o dispositivo.