INFORMAÇÃO SEGURA

Você nunca sabe o que pode estar por trás da sua tela.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 1: POLÍTICA DE TI

A **Política de Utilização de Recursos de TI** estabelece os critérios para uso dos recursos da Tecnologia da Informação, disponibilizados pela Telemont para o exercício das diversas atividades desenvolvidas pelos seus colaboradores no ambiente corporativo. Este procedimento aplica-se a todos que utilizam estes recursos de TI e/ou tenham acesso ao e-mail ou à internet.

FIQUE LIGADO!

A TI nunca irá solicitar o usuário ou senha do colaborador. Sempre verifique se algum e-mail recebido sobre uma política ou procedimento da TI foi enviado por um gestor local da filial ou canal oficial da Telemont. Caso negativo, informe imediatamente o gestor ou a área de Segurança da Informação da empresa, através do e-mail **cybersecurity@telemont.com.br**.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 2: O QUE É FISHING OU PHISING?

Fishing, que significa pesca, é a **tentativa digital de roubar dados pessoais da vítima**, como senhas, números de documentos ou cartões de crédito, endereços, dentre outras.

O objetivo do fraudador é utilizar os dados roubadas para obter vantagens financeiras como transferência eletrônica de valores, realizar compras pela internet com os dados do cartão roubado ou, até mesmo, contratar serviços como planos de telefonia, celular e televisão a cabo.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 3: TIPOS DE FISHING

Existem hoje 3 tipos de fishing, são eles: **Spear, Smishing e Vishing**.

Spear: é um tipo específico direcionado para um grupo selecionado de usuários ou departamentos da empresa, onde o criminoso estuda muito bem quem será atacado, entendendo o seu comportamento. A mensagem falsa utiliza recursos gráficos e de conteúdo que aumentam sua relevância e credibilidade.

Smishing: é um fishing que utiliza o envio de SMS para encaminhar URL's falsas para o usuário que, ao clicar no link, tem seus dados coletados pelo site acessado, bem como todos os dados existentes em seu smartphone.

Vishing: é um fishing que utiliza o voice, em que, através de uma ligação telefônica, o criminoso passa-se por um atendente de marketing para roubar os dados pessoais.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 4: BLOQUEAR O COMPUTADOR

Uma dica importante é **bloquear o computador ao se ausentar do posto de trabalho** para que ninguém tenha acesso aos seus dados.

Imagine que você está trabalhando em uma proposta de milhões de reais para a sua empresa. Em um momento, você sente sede e se levanta para pegar um copo d´água, se afastando do computador.

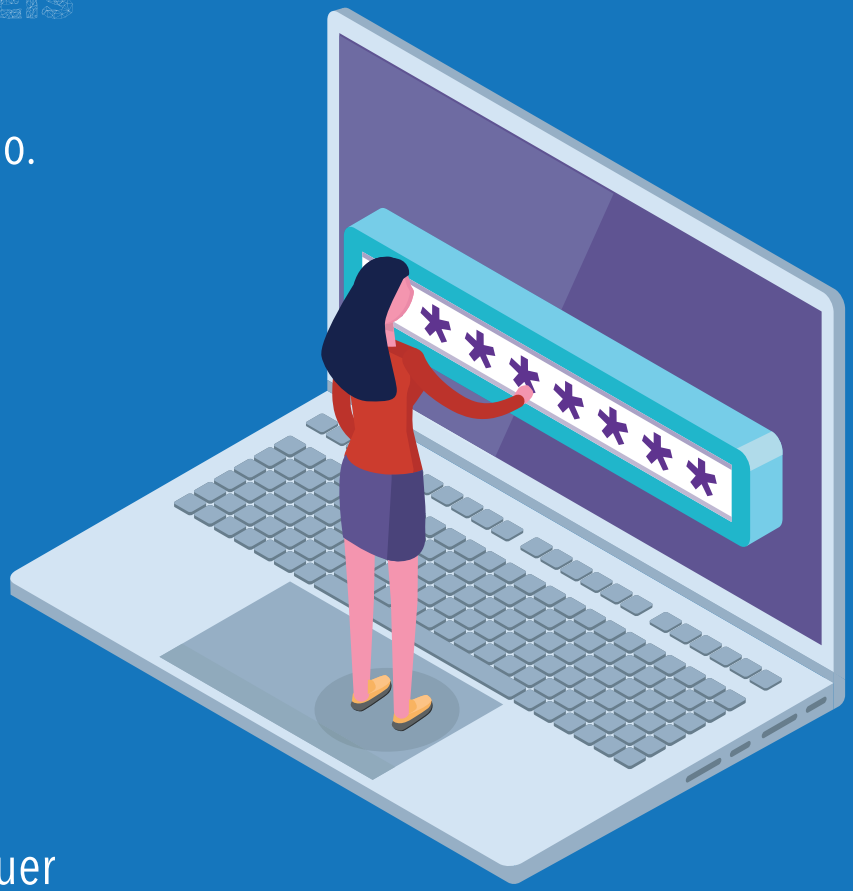
Você estava distraído e não se preocupou em bloquear sua máquina. Nesse momento, alguém com más intenções poderá se aproveitar dessa brecha para colher informações, danificar seu projeto ou alterar dados. Isso terá um impacto negativo no trabalho desempenhado por você.

Uma medida tão simples e que pode evitar problemas, afinal é melhor prevenir do que remediar, certo?

TELEMONT

INFORMAÇÃO SEGURA

#DICA 5: SENHAS PESSOAIS E INTRANSFERÍVEIS



Nunca disponibilize logins e senha, mesmo para colegas de trabalho.

Se você fornece seus dados pessoais para alguém, é preciso ter em mente que esta pessoa poderá utilizar esses dados para realizar qualquer ação.

Sendo assim, caso ele (a) utilize-os a fim de roubar informações, danificar sistemas ou cometer infrações, você não terá como provar que não foi o infrator.

Nem todos trabalham com acesso as mesmas informações, o que quer dizer que talvez você possua informações que são confidenciais e que não devem ser compartilhadas com outros membros da empresa.

Pense nisso e seja consciente!

TELEMONT

INFORMAÇÃO SEGURA

#DICA 6: DESLOCAMENTOS

Tenha atenção ao falar sobre a empresa, cliente ou negócios em locais públicos, como táxis e elevadores, por exemplo.

É de extrema importância tomar este cuidado, pois sem saber, você pode fornecer informações confidenciais e importantes da sua empresa para terceiros. Confira o exemplo no quadro ao lado e entenda.

Pense nisso e seja consciente!

Pense que você está no elevador com um colega de trabalho, conversando sobre a nova proposta de negócio que a empresa onde trabalham recebeu da empresa X. Nesse momento, o elevador para e duas pessoas entram. Vocês continuam conversando sobre a proposta, mencionando o nome da empresa X, falando sobre temas como projeto e preços, dentre outros.

O que você não poderia prever é que as duas pessoas que entraram no elevador eram nada mais, nada menos do que funcionários de uma empresa concorrente, que utilizaram as informações fornecidas ingenuamente por vocês para fazer uma contraproposta para a empresa X. Com isso, eles ganharam o projeto que seria da sua empresa, resultando em um grande prejuízo financeiro.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 7: REDES SOCIAIS

UTILIZAR AS REDES SOCIAIS COM SEGURANÇA, NÃO DISPONIBILIZANDO INFORMAÇÕES SIGILOSAS OU FAZENDO CONTATO COM DESCONHECIDOS.

Hoje em dia, cibercriminosos utilizam as redes sociais para coletarem informações relevantes como trabalho, endereço, amigos e gostos pessoais, a fim de usá-las em ataques de engenharia social.

Ou mesmo para distribuir malware pelas máquinas. Sim, é possível! Já imaginou todas as suas informações pessoais disponibilizadas para terceiros, que, através da utilização dos seus acessos das redes sociais, podem realizar ameaças a parentes ou amigos?

Recentemente houve no Facebook uma campanha informando sob a criação de contas premium do Spotify, sistema de streaming de musica. Se observar o endereço utilizado, não era o original da empresa e o mesmo, ao clicar, baixava um vírus para a máquina do usuário, que roubava as informações de contas, acesso de bancos, entre outros dados.

Se a esmola é grande, sempre desconfie! Empresas não trabalham ou fornecem serviços de graça.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 8: E-MAILS

Ataques de phishing são cada vez mais frequentes e, inclusive, existe uma outra vertente desse golpe chamada de **SPEAR PHISHING**, que visa alvos específicos, em geral, funcionários de empresas visadas pelos atacantes.

Sendo assim, é fundamental que, ao receber um e-mail de um remetente desconhecido, você preste atenção ao conteúdo e aos comandos desse e-mail.

É importante ter em mente que ainda que você esteja sendo pressionado a tomar uma atitude, é sempre melhor se certificar de que se trata de um e-mail legítimo, evitando prejuízos financeiros e de reputação.

Pense nisso e seja consciente!

De acordo com o último relatório da Norton Cyber Security Insights de 2017, 62 milhões de brasileiros foram afetados por ciberataques, resultando em uma perda de US$ 22 bilhões.

E o mais alarmante é que 44% não sabiam identificar um phishing ou garantir se um e-mail era legítimo ou não.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 9: DOCUMENTOS DA EMPRESA

NUNCA FOTOGRAFE O AMBIENTE DE TRABALHO, PRINCIPALMENTE AS TELAS DE COMPUTADOR E DOCUMENTOS.

Suponha que você fotografou alguns documentos e gráficos da empresa para poder trabalhar em casa. Porém, você não sabia que seu telefone celular estava infectado com um malware, que permitia que um grupo de ciberatacantes tivesse acesso a todos os dados do seu aparelho.

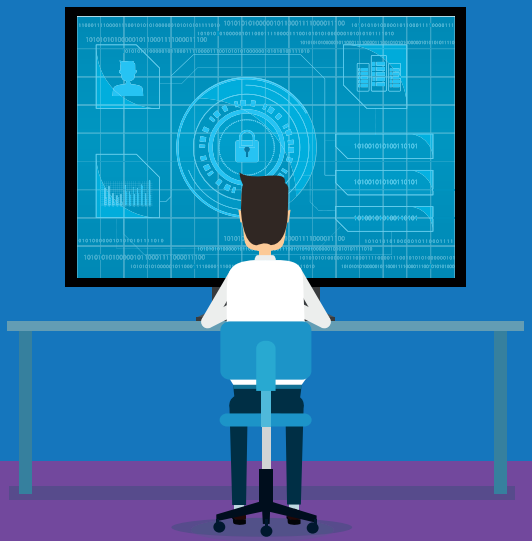
Sendo assim, à medida que você disponibilizou informações sobre a empresa no seu dispositivo, os cibercriminosos tiveram acesso a esses dados, expondo a empresa, ou seja, deixando-a vulnerável apenas por um comportamento negligente seu.

Pense nisso e seja consciente!

TELEMONT

INFORMAÇÃO SEGURA

#DICA 9: NOTIFIQUE A SEGURANÇA DA INFORMAÇÃO



REPORTE À EQUIPE DE SEGURANÇA QUALQUER PROBLEMA OU DESCONFIANÇA EM RELAÇÃO ÀS ATITUDES SUSPEITAS NO E-MAIL OU NA INTERNET.

A equipe de segurança precisa ser vista como sua aliada. Dessa forma, é extremamente importante relatar todo e qualquer tipo de problema ou suspeitas para esse time, a fim de que os especialistas fiquem cientes do que está acontecendo e possam analisar e reagir aos incidentes, diminuindo as chances de sucesso de possíveis ataques.

Pense nisso e seja consciente!

Identificou algo suspeito e precisa de ajuda?

A Telemont possui uma área especialista no assunto. Envie um e-mail para **cybersecurity@telemont.com.br**
A equipe estará a disposição.

TELEMONT

INFORMAÇÃO SEGURA

#DICA 10: SIGA AS POLITÍCAS DE EMPRESA

SIGA AS POLÍTICAS E PRÁTICAS DE SEGURANÇA DA EMPRESA, PARA QUE EXISTA UMA GESTÃO FUNCIONAL DE SEGURANÇA.

Você sabia que a Telemont possui políticas de segurança da informação e de utilização de recursos de segurança da informação?

A melhor forma de realizar o seu trabalho com segurança e protegido pela área de segurança da informação é saber o que você pode ou não fazer, dentro da rede corporativa. Caso não tenha ciência ou queira conhecer, solicite ao seu gestor regional.

Pense nisso e seja consciente!

TELEMONT