MANUAL BÁSICO DE BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

ti@commcor.com.br
si@commcor.com.br
Commcor DTVM

MANUAL BÁSICO DE BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

Objetivo

A Internet disponibiliza inúmeras possibilidades de uso e para aproveitar cada uma delas de forma segura é importante que alguns cuidados sejam tomados. A finalidade deste Guia visa ajudar os usuários a proteger seus dispositivos eletrônicos contra ataques cibernéticos e/ou roubo de dados pessoais. Algumas atitudes simples podem evitar grandes problemas!

Confira abaixo algumas dicas e recomendações que a Commcor preparou para que você possa navegar com segurança nas plataformas digitais.

1. Composição de senhas, armazenamento, alteração e assinatura eletrônica:

É através de contas e senhas que os sistemas conseguem identificar quem você é, confirmar sua identidade e definir as ações que você poderá realizar. Assim, listamos alguns cuidados a serem seguidos para proteger suas credenciais:

- Use senhas bem elaboradas, com grande quantidade de caracteres e que não contenham dados pessoais como nomes, sobrenomes, datas comemorativas, números de documentos, placas de carros, números de telefones e similares;
- Se for possível utilize 02 (dois) fatores de autenticação (SMS, token, e-mail, etc.);
- Mantenha sua senha segura fazendo a troca no mínimo a cada 90 (noventa) dias;
- Ative a proteção por senha ou biometria em seus dispositivos móveis e computadores;
- Não anote sua senha e nem a compartilhe com outras pessoas;

IMPORTANTE: Ninguém da Commcor irá solicitar à você sua senha. Fique atento!

2. Glossário

Antimalware: Ferramenta de detecção que procura anular ou remover os códigos maliciosos de um computador;

Antivírus: Ferramenta desenvolvida para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos;

Backup: Cópias de segurança dos dados de um dispositivo ou local de armazenamento para outro. Tornando o dado redundante.

Filtro Antispam: Ferramenta que permite separar e-mails de acordo com regras pré-definidas. Utilizado tanto para o gerenciamento das caixas postais como para a seleção de e-mails válidos dentre os diversos spams recebidos;

Firewall: Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;

Phishing: Tática de enganar as pessoas com o objetivo de obter informações pessoais como números de conta, senhas de acesso, de cartões, são os mais comuns;

Spam: Palavra comumente utilizada para se referir aos e-mails não solicitados, que normalmente são enviados em larga escala.

3. Proteja o seu computador

Os computadores são os nossos melhores aliados na hora de trabalhar, estudar e executar outras tarefas. Por isto, mantê-lo seguro é essencial para mitigar os riscos envolvidos no uso da Internet. Abaixo algumas informações importantes para manter o seu computador protegido:

a. Atualizações

Não esquecer de checar suas as atualizações periodicamente. É importante manter o computador com a versão mais recente do sistema operacional e de todos os programas instalados, tais atualizações irão corrigir falhas e brechas de segurança nos sistemas.

b. Ferramentas de proteção

Utilize e mantenha atualizado os mecanismos de segurança como Filtro Antispam, Antimalware e Antivírus. Possuir um antivírus atualizado é uma das melhores saídas para obter uma proteção eficaz.

c. Firewall

Assegure-se de ter um firewall. Firewall consiste em uma barreira de proteção usada para bloquear o acesso de conteúdo malicioso. A maioria dos sistemas operacionais já possuem um software com essa funcionalidade por padrão, mas lembre-se de mantê-lo ativo, isso criará uma zona segura entre sua rede e a internet.

d. Não instale softwares suspeitos

Evite fazer downloads de aplicativos de fabricantes desconhecidos, para casos em que realmente necessite, checar se há avalições de outras pessoas sobre o produto. No entanto na dúvida, não instale. Os programas podem estar infectados e conter malwares que podem roubar dados do seu computador. Opte por aqueles softwares de empresas que você já conhece, faça download apenas de sites oficiais.

e. Atenção aos downloads

Fique atento as fontes fornecedoras quando for realizar downloads de softwares ou outros downloads como filmes, músicas, livros e fotos, eles também podem trazer problemas ao seu computador, por isso recomendamos que só faça downloads de sites confiáveis e renomados.

f. Se precisar de manutenção

Caso o seu computador necessite de manutenção, busque atendimento especializado e oficial e sempre que possível faça backup dos seus dados antes de enviá-lo, lembrando de jamais permitir a instalação de programas não genuínos.

4. Proteja seus dispositivos móveis

Os dispositivos móveis (celulares, smartphones e tablets) se tornaram uma parte relevante de nossas vidas, além de serem importantes meios de comunicação que permitem guardar dados e informações pessoais, acessar e-mails, fotos, redes sociais, internet banking, dentre outras funções que facilitam nosso dia a dia. Contudo assim como seu computador, os seus dispositivos móveis também podem ser alvo de atividades maliciosas. Algumas dicas para proteger o seu dispositivo móvel:

a. Atualizações

Novamente, semelhante aos computadores, não se esqueça de checar as atualizações constantemente. É importante manter o seu mobile seguro com a versão mais recente do sistema operacional e de todos os apps instalados.

b. Não instale aplicativos suspeitos

Evite fazer downloads de aplicativos de terceiros de fontes desconhecidas. Na dúvida, não instale. Para se proteger, faça download apenas de fontes confiáveis, como a App Store e Google Play.

c. Senha, biometria e reconhecimento facial

Para evitar que pessoas não autorizadas tenham acesso as suas informações de forma rápida, ative o bloqueio da tela inicial. Essa simples ação pode evitar grandes transtornos.

d. Interfaces de comunicação

Deixe as interfaces de comunicação como bluetooth, NFC e WiFi desabilitadas, habilite somente quando for necessário.

5. Ações em caso de perda ou furto

Altere as senhas que possam estar armazenadas no aparelho e /ou no computador, por exemplo: redes sociais, e-mail, aplicativos de compras e armazenamento em nuvem. Atenção aos cartões de crédito adicionados no

mobile para compras indevidas ou desconhecidas, por prevenção os cartões podem ser bloqueados junto a operadora.

a. Localização e Bloqueio Remoto

Os dispositivos móveis mais modernos possuem a tecnologia que possibilita ser bloqueado remotamente por meio de serviços de geolocalização (isso pode ser bastante útil em casos de perda ou furto), consulte o fabricante.

6. Atenção ao acessar redes públicas de Wi-Fi:

É comum encontrar estabelecimentos como restaurantes e bares que oferecem rede Wi-Fi gratuita. Essa comodidade oferecida pelas empresas à seus clientes é uma forma de se distrair durante a espera ou ser um atrativo do estabelecimento, mas saiba que essa rede Wi-Fi pública não disponibiliza a mesma segurança que uma rede privada, sendo mais fácil para pessoas mal-intencionadas capturar seus dados.

A dica mais rápida e direta neste assunto é: NÃO ACESSE! Ou evite esse tipo de acesso . Se for uma emergência, tente ser breve e acesse apenas o necessário. Caso queira ou precise acessar dados confidenciais, como seu banco ou informações de trabalho, dê preferência em utilizar seu celular como um roteador Wi-Fi e compartilhe os dados por ele, transformando a rede aberta em privada e limitando o acesso apenas para seus dispositivos (notebook por exemplo).

Em caso de atividades de trabalho, você também pode consultar a equipe de TI da sua empresa se é possível viabilizar uma conexão VPN (rede virtual privada) para ser acessada durante o uso de Wi-Fi longe do escritório.

7. Proteja os dispositivos físicos

Em virtude do tamanho reduzido, do alto valor financeiro e do status que representam, notebooks e celulares, unidades removíveis e outros dispositivos móveis, são facilmente roubados e/ou furtados com todos os dados que eles contêm. Mantenha seus dispositivos seguros com você e adequadamente armazenados, especialmente ao usá-los em lugares públicos como restaurantes, cafeterias ou deixá-los em ambientes como carros.

8. Cuidados com os links

Tenha muito cuidado com os links que você clica, principalmente os que aparecem em e-mails, redes sociais e anúncios da web. Histórias diferentes, curiosas e engraçadas demais podem ser uma armadilha para ataques cibernéticos, assim como ofertas discrepantes de produtos, promoções exorbitante e similares. Use o bom senso e pesquise sobre o assunto com o intuito de arranjar uma fonte confiável.

9. Atenção aos e-mails e anexos falsos

Não clique em links ou anexos enviados por endereços virtuais desconhecidos e muita atenção nos remetentes conhecidos enviando mensagens sobre oportunidades, prêmios, super promoções, dinheiro e rastreamento de encomendas. Muitas vezes essas mensagens foram corrompidas e caem na sua caixa de entrada como um golpe de "**phishing"**!

IMPORTANTE: Um golpe de "phishing" é um e-mail que parece legítimo, mas na verdade é uma tentativa de obter suas informações pessoais, incluindo suas senhas e dados bancários. A armadilha acontece quando você acessa o link recebido nessas mensagens falsas e insere os seus dados sensíveis/pessoais como nome completo, telefone, CPF e números de contas bancárias.

10. **Ao usar computadores de terceiros:**

Certifique-se de fechar a sua sessão (logout) ao terminar de usar dispositivos de pessoas terceiras. Caso acesse sites que usem senhas pessoais procure sempre, utilizar opções de navegação anônima, limpar o histórico e não permita que suas senhas sejam memorizadas pelo navegador Web. Além disso, evite utilizar serviços como transações bancárias ao usar máquinas de terceiros e seja cuidadoso ao conectar mídias removíveis, como pen-drives, celulares e tablet.

11. **Evite compartilhar informações pessoas e relacionadas ao trabalho em redes sociais**

Compartilhar em redes sociais muitos detalhes sobre suas responsabilidades e atividades no trabalho, pois suas atividades, rotinas e informações de contato podem atrair golpistas e pessoas mal-intencionadas. Eles podem aproveitar essas informações para enviar à você mensagens de **phishing** que parecem legítimas e atrativas, podendo resultar em transtornos futuros.
O compartilhamento de informações pessoais em redes sociais deve ser evitado ao máximo, como local de trabalho, escola do filho(a) e principalmente a divulgação aberta, para pessoas que não fazem parte do seu ciclo de convivência (amigos, familiares...).

Essas são somente algumas dicas e orientações que a equipe de TI da Commcor acredita ser útil para colaborar com uma navegação na internet que seja segura para nossos Clientes e Parceiros. Em caso de dúvidas, estamos à disposição para ajudá-lo, entre em contato com a gente através dos canais abaixo:

ti@commcor.com.br

si@commcor.com.br