Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Cuidados necessários ao utilizar os computadores do trabalho

Edição nº23
Maio/2022

A segurança em meio à internet deve ser redobrada dentro de uma empresa. Em primeiro lugar, as informações têm uma importância e uma carga de sigilo muito maior do que na sua casa. Em segundo lugar, é como se cuidássemos de algo muito mais importante para a empresa como um todo do que só para nós. Se você utiliza o computador da empresa para atividades pessoais, Saiba que misturar a vida pessoal com a profissional não é uma prática muito bem vista pelos especialistas em cibersegurança. É recomendável evitar o uso particular de computadores da empresa onde você trabalha como prevenção contra possíveis problemas como ataques de cibercriminosos, vírus, tentativas de phishing e ransomwares.

Manter e respeitar o bom uso do computador corporativo é de responsabilidades do colaborador. O mau uso do computador pode envolver diversos aspectos, desde a parte de hardware, constituída pelo mouse, teclado, monitor e gabinete, até instalação de softwares. O mau uso do computador também se refere a utilização indevida da internet da empresa. Sob esse aspecto, inclui-se o acesso a sites que não são relevantes aos assuntos da companhia e de programas peer to peer, também conhecidos como P2P, que possibilitam que usuários se conectem entre si para baixar todo tipo de arquivo, desde música até filmes completos. Essa prática pode prejudicar a banda de internet e a rede da empresa. Isso sem contar que, na maioria das vezes, esses arquivos baixados podem conter vários tipos de malware.

De forma geral, após algum tempo de empresa, as pessoas começam a se sentir mais confiantes e confortáveis. Com isso, elas passam a tratar o computador corporativo como se fosse seu computador doméstico. Porém, é importante ter em mente que a empresa disponibiliza o uso do computador apenas para melhorar o desempenho de cada colaborador. Isso considerando a execução de seu trabalho, e não de tarefas de âmbito pessoal.

Seguem algumas dicas de melhores práticas de uso do computador da empresa:

- Não armazenar dados ou imagens pessoais no computador: mesmo que você esteja habituado ao computador e que o use com frequência, lembre-se que se trata de um instrumento de trabalho. Outros funcionários podem, eventualmente, utilizar o mesmo dispositivo;
- Não instalar softwares sem a autorização da TI: em muitos computadores, a instalação de novos programas é desabilitada. Caso seja importante instalar um novo software, é preciso cuidado para não infectar a máquina com algum tipo de malware. O melhor a fazer é entrar em contato com a TI e relatar a necessidade;
- Mantenha o computador sempre limpo e evite comer próximo a ele. Isso porque migalhas podem prejudicar o bom funcionamento do teclado e até mesmo o da ventoinha da CPU;
- Nunca baixe programas sem autorização do departamento de TI. Antes de fazer o download de qualquer software, é importante conversar com o técnico responsável. Assim, ele poderá verificar se o programa realmente é necessário à execução do trabalho. Isso além de consultar a confiabilidade da fonte;
- Saia dos sistemas clicando em "Logout", "Sair" ou equivalente: ao acessar seu e-mail ou sistema no qual você esteja trabalhando, clique no botão ou link de nome "Logout", "Logoff", "Sair", "Desconectar" ou equivalente para sair do site. Pode parecer óbvio, mas muita gente simplesmente fecha a janela do navegador ou acessa outro endereço a partir dali. Agir assim não é recomendado porque o site não recebeu a instrução de encerrar o seu acesso naquele momento, de forma que outra pessoa poderá reabrir a mesma página logo em seguida e acessar as suas informações;
- Nunca conecte dispositivos portáteis de armazenamento de dados não confiáveis: Muitos malwares infectam as máquinas somente com o ato de "espetar" o dispositivo na USB do computador. Esse golpe é muito praticado e pega muita gente que acha que é uma vantagem achar um pendrive na rua ou que ganhou um pendrive de alguém desconhecido;
- Nunca baixar arquivos torrent, ares, torch e similares: essas atitudes consomem banda de internet para assuntos não relacionados a empresa, abrem portas de acesso a ataques hackers e trazem vírus a rede junto aos arquivos.

Na maioria das vezes, o departamento de TI precisa educar, monitorar e, ocasionalmente, punir usuários pelo mau uso das ferramentas da empresa. Para isso, ele adota políticas de segurança para o ambiente de TI. Essa prática inclui desde a liberação de acessos junto à rede até seu bloqueio total. Contudo, o bloqueio só costuma ocorrer em casos extremos. Ou seja, quando o usuário ultrapassa os níveis pré-definidos de notificações recebidas pelo mau uso das ferramentas.

Fique ligado: no próximo mês, falaremos sobre
Cuidados ao realizar operações financeiras