

Nome: Rafael Gonçalves Rodrigues da Cunha Vinhas
Curso: Segurança da informação – Fundamentos - 2018
Grupo: B

Cartilha de Segurança da Informação

Dicas de segurança da informação para ambiente residencial:

- 1) Compras em ambiente virtual: antes de comprar qualquer produto ou serviço pela internet, é importante certificar-se da reputação da empresa. Existem diversos sites que recebem opiniões de pessoas que já compraram anteriormente e avaliaram o serviço. É importante sempre verificar o ambiente de compra e se o endereço do site é iniciado com <https://>. Algumas instituições bancárias já oferecem cartões de crédito virtuais aos seus clientes, o que permite a utilização do número de cartão de crédito apenas uma vez, evitando assim o roubo dos dados do cartão.
- 2) Não acesse sua conta bancária através de redes abertas ou de computadores estranhos, como em lan-houses, por exemplo, para evitar o risco de roubo de senha através da interceptação dos dados na rede ou através de programas maliciosos no computador.
- 3) Não compartilhe notícias, áudios ou vídeos sem certeza de sua procedência. Mensagens alarmistas, de fontes desconhecidas, sem identificação de autoria e sem data normalmente são fake news. Essas notícias falsas podem ser utilizadas para disseminar boatos sobre pessoas ou instituições, espalhar vírus, além da notícia falsa em si, que pode causar danos à sociedade disseminando mentiras sobre vacinação, por exemplo, dentre outras.
- 4) Não forneça seus dados pessoais por e-mail ou telefone. Golpistas utilizam da engenharia social, se passando por instituições bancárias, instituições públicas ou comerciais para descobrir informações pessoais.
- 5) Se utilizar wi-fi em sua residência, procure sempre utilizar a configuração WPA2, e uma senha forte. Nunca deixe sua rede wi-fi aberta.

Dicas de segurança da informação para o ambiente institucional:

- 1) Nunca forneça sua senha pessoal de acesso à Intranet para outra pessoa.
- 2) Evitar repetir a mesma senha para diferentes acessos. Ter uma única senha nos deixa muito vulneráveis, pois no caso de roubo da senha será fácil para o invasor acessar todas suas contas.
- 3) Manter sempre um backup para evitar a perda de informações que podem acontecer em caso de acidentes físicos, infecção por vírus de computador, equívoco na hora de apagar arquivos do HD dentre outras causas. Existem diversas modalidades de backup, como backup na nuvem, HD's, CD's ou DVD's, Pen Drivers, cada modalidade apresenta vantagens e desvantagens e deve-se analisar o tipo de backup mais adequado para uma situação específica.
- 4) Mantenha sempre o seu sistema operacional atualizado. As ameaças estão sempre evoluindo e os sistemas operacionais oferecem atualizações periódicas para anular vulnerabilidades do sistema.
- 5) Assim como o sistema operacional, é importante manter um antivírus atualizado. As dicas 4 e 5 são importantes tanto no ambiente doméstico como no institucional.
- 6) Realizar treinamentos periódicos dos colaboradores, para estarem sempre preparados para detectarem e neutralizarem ameaças.

Bibliografia:

<https://procon.campinas.sp.gov.br/compras-pela-internet-procon-d-dicas-seguran>

<https://cartilha.cert.br/redes/>

<http://marcusmarques.com.br/pequenas-e-medias-empresas/dicas-seguranca-da-informacao-empresa/>

<https://www.security.ufrj.br/category/dicas/>