Valéria Reani: Segurança da informação e proteção de dados

Em isolamento social por causa da pandemia do novo coronavírus, o recurso da internet vem crescendo para finalidades como o teletrabalho, a comunicação com parentes, amigos e colegas, a busca por informações e momentos de lazer no consumo de músicas e vídeos. Com isso, é preciso aumentar também os cuidados para evitar acessos indevidos, entrada de vírus ou golpes aplicados pela web.

A grande ferramenta que possibilita uma mobilidade real para transportar o trabalho para qualquer lugar e? o laptop, ou notebook. Hoje esses computadores porta?teis possuem as mesmas funcionalidades e capacidades dos computadores de mesa, mas com a vantagem da portabilidade, acesso à internet sem fio (wi-fi) e baterias com capacidade para horas de funcionamento conti?nuo (LOPES, 2008).

A banda larga proporciona a mobilidade e a comunicac?a?o via Skype ou outras plataformas. Ale?m da possibilidade de tornar a conversa a? dista?ncia mais realista, como as por videoconfere?ncia, que tambe?m podem ser de alta resoluc?a?o.

Nesse contexto, a pergunta é: como o colaborador pode garantir a segurança da informação em teletrabalho? (1)

1 — Verifique seu firewall
Em informática, um firewall (em português: parede de fogo) é um dispositivo de uma rede de computadores, na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associado a redes TCP/IP.

Certifique-se de que o seu firewall está ativado para manter os *cibercriminosos* fora. Além disso, se você não quer que seus arquivos estejam visíveis em outro computador, desative por completo a opção de compartilhar documentos.

2 — Backup dos seus dados
Fazer o backup dos seus dados protege sua informação no caso de uma pane no computador ou falha elétrica. Também ajuda se você cair na armadilha de um *ransomware**, que criptografa os seus dados confidenciais. Você pode fazer o backup manualmente através da transferência de documentos importantes para um disco rígido externo. Se você não tem uma quantidade significativa de dados para armazenar, use um serviço como o Dropbox, em que você recebe 2 GB de armazenamento gratuito.

*Obs.

Ransomware é um tipo de malware (software malicioso) que afeta sistemas informáticos ou redes inteiras de computadores, tornando alguns dos dados disponíveis no equipamento totalmente inacessíveis, sendo que somente poderão ser desbloqueados a partir do pagamento de um resgate (*ransom*) por parte do usuário.

3 — Sites desonestos
Ainda que seja difícil saber se uma página web é confiável ou não, existem certas medidas que podemos tomar para melhorar nossas habilidades de identificação. Por exemplo, procure um bloqueio verde na barra de navegação e o prefixo do código "https://" no início da URL quando visitar sites em que é necessário introduzir os seus dados de cartão de crédito. Tenha cuidado ao fazer compras em sites do exterior e não clique em links enviados por e-mail, pois isso fará com que você seja direcionado ao site em si.

4 — Informações confidenciais
Não importa o site, sempre tenha cuidado com o tipo de informação que você disponibiliza. Embora seja de conhecimento geral, não custa nada reiterar que você não deve passar dados de cartão de crédito e seguro social, a menos que você confie no site completamente. Também é importante ser cuidadoso com seus perfis nas redes sociais. Revelar informações inocentes como, por exemplo, o nome do seu animal de estimação ou o nome de solteira da mãe pode resultar no roubo da sua identidade, já que usa esses mesmos dados em algum outro site para a verificação

5 — Senhas
Senhas podem ser insuficientes, para garantir a segurança de suas contas é necessário habilitar a verificação em duas etapas.

6 — Conexões seguras
Use sempre conexões seguras, como "https:" para acesso a sites web e remoto à empresa em que você trabalha, por exemplo.

7 — Atualização de software
Além de ficar em casa e se proteger, lembre-se de proteger também seus softwares mantendo-os atualizados e instalando mecanismos de segurança.

8 — NÃO abrir e-mails de desconhecidos
Nunca abra um e-mail de uma fonte desconhecida ou suspeita e, definitivamente, nunca abra os anexos. Também tenha cuidado com e-mails estranhos enviados por conhecidos, já que a conta desse contato pode ter sido *hackeada*. Nesse caso, apague a mensagem e o avise imediatamente de que sua conta pode ter sido comprometida. Isso irá ajudá-lo a evitar golpes de hackers e *phishing,* e que você seja um alvo.

A segurança do seu computador pessoal é, provavelmente, algo com que você já esteja lidando por um longo tempo. Se você atualiza o seu antivírus e cria senhas fortes para suas contas online, alterando-as regularmente, você tem todas as suas bases cobertas.

Outrossim, vale lembrar que a adoção do trabalho remoto, em temos de crise da Covid-19, pode trazer uma série de riscos de *cibersegurança* às empresas mais desavisadas. "O coronavírus não apenas está colocando a saúde das pessoas em cheque, como também está sendo usado como isca por cibercriminosos para propagação de malwares. Se por um lado o

aumento do trabalho remoto ajuda a proteger a saúde dos trabalhadores, por outro, criminosos tentam tirar proveito do interesse por informações sobre a doença, ocultando arquivos maliciosos em documentos supostamente relacionados a este surto. Enquanto estivermos preocupados com as ameaças à saúde, é possível que surjam mais e mais golpes", explica Dmitry Bestuzhev, diretor da equipe de pesquisa e análise para a América Latina da Kaspersky. (2)

Nesse contexto, vale o questionamento de como as empresas devem reduzir os riscos de seus colaboradores no home office e garantir a segurança da informação em teletrabalho.

Eis algumas dicas da Kaspersky: (3)

— Forneça uma VPN (Rede Privada Virtual) para as equipes se conectarem com segurança à rede corporativa;

— Restrinja os direitos de acesso dos usuários que se conectam à rede corporativa;

— Eduque as equipes sobre os perigos de responder mensagens não solicitadas e acessar links ou baixar arquivos com origem desconhecida.

— Instale as atualizações mais recentes dos sistemas operacionais e de aplicativos.

— Proteja todos os dispositivos da empresa (incluindo smartphones, laptops e tablets) com uma solução de segurança adequada.

A telemedicina
A telemedicina não é exatamente uma novidade. A prática permite que médicos prestem atendimento à distância por meio de telefones, computadores e *tablets*, e tem sido discutida há bastante tempo. No Brasil, o Ministério da Saúde publicou Portaria Nº 467, de 20 de março de 2020, em resposta emergencial ao novo coronavírus, para complementar a Resolução CFM nº 1.643/2002 (4), de agosto de 2002, que regulamenta a telemedicina em território nacional.

"Dispõe, em caráter excepcional e temporário, sobre as ações de telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no artigo 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19". (5)

Nesse contexto, a pandemia do novo coronavírus abriu uma exceção na rotina das consultas médicas. Agora, quem precisar pode ser atendido à distância por um médico. A telemedicina foi autorizada pelo Ministério da Saúde em caráter de emergência e vai funcionar apenas enquanto houver recomendação de isolamento social

Os serviços, porém, não se restringem aos ligados à Covid-19, mas abrangem todas as especialidades médicas, que vão desde uma orientação pediátrica até uma consulta com um cirurgião plástico. Não existe uma lista restritiva de especialidades imposta pelo ministério e nem pelo Conselho Federal de Medicina (CFM).

Mas, mesmo sem proibição a qualquer tipo de atendimento, a orientação é que o atendimento médico online seja indicado especialmente para os idosos, que são hoje o maior grupo de risco para o coronavírus.

Privacidade e segurança das informações em telemedicina
E é preciso estar atento a algumas questões depois dessa consulta. No prontuário eletrônico é preciso constar data, hora e meio de comunicação utilizado, porque é um atendimento e existe responsabilidade civil do médico. Por segurança, é importante que o paciente guarde essas informações. Caso o médico tenha a tecnologia específica, como a assinatura eletrônica, é possível emitir, inclusive, um atestado à distância.

A telemedicina é uma inovação poderosa, com potencial para a privacidade do paciente (a LGPD terá enorme papel nesse sentido).

Referência bibliográfica
LOPES, Airton. A Nova Safra de Laptops. Em Info Exame. Sa?o Paulo, n.265, p.52-57, 2008.

(1) Dicas para manter seu computador seguro. Acesso em https://www.kaspersky.com.br/blog/6-dicas-para-manter-seu-computador-pessoal-seguro/1637/

(2) e (3) Coronavírus: dicas para empresas adotarem home office , acessado em 15/04/2020: https://www.kaspersky.com.br/blog/coronavirus-dicas-home-office/14497/

(4) Resolução CFM nº 1.643/2002 disponível em https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643

(5) Diário oficial da União Portaria 467 de 20 de março de 2020, acessado em 15/04.2020 disponivel em http://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996

Date Created
22/04/2020