Recomendações de Segurança para Trabalho Remoto

O alerta do novo Coronavírus está levando as empresas, em diversos países, a tomarem medidas como o teletrabalho para evitar o contágio. Há uma ampla adesão e os profissionais devem permanecer sempre atentos às ciberameaças, pois os cibercriminosos continuam com suas atividades maliciosas criando malwares e sites fraudulentos sobre o COVID-19.

No entanto, os níveis de proteção nos ambientes domésticos são inferiores aos ambientes profissionais e, por este motivo, criminosos podem tirar proveito desses tipos de situações para lançar ataques que colocam em risco usuários e empresas. Assim, seguem recomendações relacionadas ao ambiente para o teletrabalho, para o mesmo seja realizado com maior segurança:

1. **Revisar as senhas**: é essencial estabelecer senhas robustas (mínimo 10 (DEZ) caracteres que combinem letras maiúsculas e minúsculas, números e símbolos) para acessar recursos profissionais, como e-mail ou aplicativos de trabalho.

2. **Proteger-se de *phishings***: evite clicar em links que pareçam suspeitos e fazer o download apenas de fontes conhecidas. É essencial lembrar que as técnicas de *phishing* são cada vez mais sofisticadas; portanto, no caso de receber um e-mail com uma solicitação incomum, é necessário verificar minuciosamente os dados do remetente para garantir que ele seja de um colega de trabalho ou de fontes confiáveis, e não de cibercriminosos.

3. **Reforçar as prevenções ao utilizar redes públicas**: evite utilizar redes Wi-Fi públicas de aeroportos, restaurantes, entre outros estabelecimentos e locais públicos, inclusive para acesso remotos aos recursos da SEFAZ, é imprescindível reforçar as medidas de proteção, já que essas conexões não são seguras e podem ser até mesmo um foco de ataques por parte dos cibercriminosos.

4. **Instalar e atualizar antivírus**: utilize software de antivírus e mantenha as atualizações em dia para proteção mínima contra ameaças de vírus e outros malwares.

5. **Atualizações do Sistema Operacional**: mantenha o sistema operacional licenciando e atualizado com no mínimo as atualizações críticas e de segurança.

6. **Bloquear o computador:** bloqueie o acesso ao computador se estiver trabalhando em lugar compartilhado garantindo o sigilo das informações.

7. **Evitar sites não seguros**: evite entrar em sites não profissionais durante o período de trabalho.

8. **Browsers Atualizados**: utilize navegadores (Internet Explorer, Google Chrome, Firefox) em suas versões mais atuais.

9. **Softwares piratas ou não licenciados**: evite utilizar softwares piratas, além de crime, podem causar danos a instituição: infecção do computador com malwares, comprometimento da segurança dos dados, capturas de senhas.

10. **Programas em desuso**: remova programas que você não utiliza mais. Programas não usados tendem a ser esquecidos e a ficar com versões antigas podendo serem explorados por criminosos.