Introdução

A possibilidade de realizar o trabalho em casa, algo que era uma realidade distante para a maioria das pessoas, por conta das ações de prevenção a COVID-19, forçadamente teve de se materializar. Entretanto, como se proteger dos também conhecidos como "vírus" e outras ameaças do mundo cibernético que vieram junto com essa ação?

Do dia para a noite, muitas empresas tiveram que redesenhar sua infraestrutura e adaptar a segurança, o acesso e a geração dos seus dados e informações por conta da obrigatoriedade do isolamento social e tiveram que adotar o trabalho remoto às pressas, sem tempo de investir em tecnologia, dar o treinamento adequado ou disseminar políticas de segurança da informação.

Isso abriu uma grande oportunidade para o cibercrime e, para ajudar a se defender dessa ameaça, abaixo seguem algumas dicas:

Sobre o Home Office:

- Se puder, não compartilhe o computador de uso doméstico com o que vai ser usado para trabalhar;
- Sempre busque junto aos times de TI referências dos *softwares* e aplicativos homologados pela empresa;
- Certifique-se que seus computadores, *smartphones*, equipamentos de rede local e os sistemas e aplicativos estão atualizados e possuem sistemas de segurança como antivírus e *firewall* habilitados e atualizados;
- Se possível, segmente a sua rede doméstica: use uma rede exclusiva para o trabalho e outra para uso da família;
- Como procedimento vital para sua segurança e que é independente do período em que nos encontramos, NUNCA USE redes Wi-Fi públicas. Elas, além de inseguras, normalmente são criadas com o objetivo de capturar dados e roubar informações;
- Nunca deixe seus equipamentos sozinhos e desbloqueados com acesso aos sistemas da empresa. Se houver necessidade de se ausentar por um período curto de tempo bloqueie a máquina, senão, simplesmente salve seu trabalho, feche os aplicativos e sistemas e desconecte da infraestrutura do trabalho;
- Aprenda e use sem exceção aquilo que é apontado como procedimento básico em segurança da informação: cuide das suas senhas sem compartilhar elas entre conhecidos ou repetindo-as entre os sites (use senhas fortes!), aprenda a usar um sistema de duplo fator de autenticação e guarde suas senhas em um *software* gerenciador de senhas;
- Muito cuidado ao criar, armazenar e compartilhar informações da empresa, busque sempre junto as equipes de TI orientações sobre como guardar os dados e qual a política de segurança para ser seguida em caso do uso de armazenamento em servidores que não os corporativos;
- Em caso de dúvidas, entre em contato com o time de TI ou de segurança da sua empresa e peça ajuda.

Sobre o uso de smartphone:

Por ser disparadamente o meio de acesso mais usado, boa parte dos ataques são direcionados a esse tipo de dispositivo.

Até o momento, os principais golpes que apareceram usando o tema do COVID-19 foram campanhas por e-mail, mensagens de WhatsApp e até de SMS para a roubo de dados ou para a infecção com vírus nos smartphones (e computadores) das vítimas.

Também já existem relatos de que cibercriminosos estão usando a COVID-19 e a necessidade de isolamento social para aplicar golpes de engenharia social, incluindo mensagens e ligações falsas para coleta de donativos ou cobrança de serviços.

Uma constante entre os ataques tem sido as mensagens sobre a pandemia com links maliciosos espalhadas pelas redes sociais e aplicativos de comunicação instantânea, como o WhatsApp.

Entre os aplicativos falsos, os mais comuns foram os que supostamente permitiam a visualização de mapas da contaminação, mas que na realidade fazem o "sequestro" do celular da vítima ou instalam uma ferramenta para monitorar o uso do celular capturando todas as informações geradas.

Para evitar ou mitigar o seu risco ao usar o smartphone as dicas anteriores são válidas e podem ser somadas as seguintes ações:

- Não instale aplicativos fora das lojas oficiais;
- Antes de instalar alguma coisa leia as avaliações dos outros usuários e revise a lista de permissões que o aplicativo solicita;
- Revise os aplicativos instalados e desinstale aquilo que não é mais usado;
- Procure manter o sistema operacional atualizado e crie uma rotina para verificar se os aplicativos também estão em sua última versão liberada pelo desenvolvedor;
- Como o smartphone hoje centraliza e concentra boa parte de nossas vidas; seja no contexto pessoal, seja no profissional; mais do que tudo busque conhecimento e aprenda a usar as ferramentas disponíveis com segurança.

Sítios para referência e aprofundamento sobre o assunto:

https://ssd.eff.org/pt-br

https://twofactorauth.org/

https://internetsegura.br/

https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaosegura-confira-dicas-para-proteger-dados-pessoais

https://www.rnp.br/sistema-rnp/cais

http://new.netica.org.br/prevencao/

https://new.safernet.org.br/

https://www.childhood.org.br/navegacao-segura