UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

DICAS E SUGESTÕES PARA SUA SEGURANÇA ONLINE E NO USO DE FERRAMENTAS WEB

A Superintendência de Tecnologia da Informação (STI/UFES) recomenda aos servidores e alunos a leitura deste texto, que trata de sua segurança quando online (na Internet e em redes de computadores), enfatizando também a importância de sua atenção para os diversos softwares e plataformas em uso, bem como para as ferramentas de web conferencia.

A crise da COVID-19 fez com que milhões de pessoas passassem ao trabalho remoto, quando possível, por conta das políticas públicas de saúde que demandam "quarentena" e "isolamento social". Assim, as **plataformas de comunicação online** (Google Meet, Cisco Webex, Zoom, Jitsi Meet, etc.) tornaram-se ainda mais necessárias para as interações, tanto pessoais quanto profissionais.

Realizar trabalho remoto, utilizar redes de computadores, VPN, sistemas, aplicativos de celular, acessar serviços bancários e outros, realizar pesquisas no Google, acessar as "redes sociais", jogar, etc. tornaram-se atividades que fazem parte da rotina de inúmeras pessoas. **Mas, um detalhe interessante: a preocupação com a segurança online normalmente tem estado abaixo do que deveria ser, exceto quando um problema ou prejuízo já aconteceu**.

Infelizmente, é baixo o número de pessoas que classificam a segurança como o fator mais importante na tomada de decisões sobre seu computador ou seus dispositivos online. Mas, em realidade, ser **proativo** com a segurança online não deve ser um assunto tratado como "inconveniente": deve ser uma **PRIORIDADE**, sob penas de sérias consequências.

Por estas razões, objetivamente apresentamos aqui alguns tópicos que devem ser considerados quando o assunto é segurança online (sem pretensão de esgotar o assunto, evidentemente).

Inicialmente, É IMPORTANTE NOTAR QUE:

(1) Quase todos os aplicativos e serviços online são vulneráveis a serem comprometidos por ataques como "*phishing*" *, *"engenharia social"* **, *"malwares*" *** e outros, pelos quais as informações de *login, nome de usuário, conta, senhas* e outras podem ser obtidas.

(2) É praticamente impossível obter 100% de segurança online, do mesmo modo como na vida real não existe 100% de segurança no cotidiano.

(3) Mesmo com ferramentas de segurança digitais, o comportamento irresponsável e as atitudes inconsequentes dos usuários de redes, serviços, plataformas e sistemas podem comprometer praticamente quaisquer "esquemas" montados para proteção online. Por este motivo, é extremamente importante o **comprometimento dos usuários com a segurança da informação**, através de boas práticas, educação continuada, atenção constante e vigilância ativa.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Sobre as recomendações de segurança online.

É ABSOLUTAMENTE RECOMENDÁVEL QUE OS USUÁRIOS SEMPRE ADOTEM BOAS PRÁTICAS DE RESPONSABILIDADE E DE SEGURANÇA DA INFORMAÇÃO.

É importante assinalar que estas recomendações se aplicam também ao uso de VPN, às plataformas diversas de softwares, à navegação online, ao uso de e-mails e contas de acesso a serviços e sistemas, a aplicativos de mensagens, redes sociais, etc., incluindo sua casa e seu ambiente de trabalho, seja físico ou virtual (trabalho remoto). Se seu dispositivo, roteador, computador, telefone celular ou seus dados de acesso são comprometidos por um ataque criminoso ou por comportamentos inseguros de sua parte quando online, seus dados e informações estarão igualmente comprometidos, com sérias consequências.

Entre outros tópicos importantes, destacam-se:

1. O básico

Parece simples, mas realizar atualizações regulares do S.O. (Sistema Operacional) do seu computador é uma das ações mais importantes para protegê-lo. As atualizações são, muitas vezes, a forma como as empresas enfrentam um possível problema de segurança. Você pode facilmente configurar o seu sistema operacional para verificar automaticamente se existem novas atualizações e instalá-las.

2. Reuniões, palestras, eventos online e videoconferências

Como qualquer tecnologia popular, os aplicativos de videoconferência oferecem inúmeros benefícios que proporcionam aos colaboradores manter suas atividades diárias. Mas vale lembrar: eles também representam riscos para as informações compartilhadas. **Adote todas as configurações de segurança e privacidade necessárias, de acordo com o aplicativo usado e com o teor e sensibilidade de suas reuniões**. É importante que cada usuário, cada moderador, cada organizador, adote estas medidas. Em caso contrário, problemas poderão ocorrer, assim como no mundo real, quando nos descuidamos. Uma breve analogia entre o mundo real e virtual, é avaliar para quem você fornece o endereço para ingressar na sua sala. Em reuniões online, procure utilizar senha de acesso e "sala de espera" para aprovação e admissão na reunião. **Para eventos abertos ao público, recomendamos usar da facilidade de transmissão ao vivo para as plataformas Youtube ou Facebook e somente os convidados e palestrantes estarem presentes na sala de webconferência.** A presença de um moderador para fazer a interação dos palestrantes e as dúvidas inseridas no bate-papo pelo público externo é fundamental para o sucesso do evento. É recomendável que as reuniões em salas pessoais sejam bloqueadas 10 minutos após o início da reunião. Isso impedirá que pessoas indesejadas entrem nas reuniões. Em diversos aplicativos, quando os convidados tentarem entrar na sua reunião bloqueada, você verá uma indicação no aplicativo de que eles estão esperando para serem admitidos. Você poderá decidir se deseja admitir esses convidados na reunião ou deixá-los permanecer no "lobby" ou sala de espera.

Em relação ao Google Meet, recomenda-se a leitura atenta do texto **"Segurança e privacidade para a educação no Meet**", contido em: https://support.google.com/a/answer/9822731?hl=pt-BR Note-se especialmente o tópico referente às "**Medidas de Combate ao Abuso"**.

3. Não clique indiscriminadamente em qualquer link

O Google detecta milhares de novos sites maliciosos todos os dias. Há sites legítimos que foram invadidos e também aqueles que são projetados para infectar seu computador com programas maliciosos e *malwares****. **Seja sempre cauteloso com os links em que você clica e com os sites que você visita**. Lembre-se de passar o mouse sobre os links, para que você possa rever o endereço completo antes de clicar, certificando-se de que o link aponta para o site correto indicado. Finalmente, mantenha sempre o firewall e antivírus ativos em seu computador e na sua rede. Sempre atualize **o antivírus.** E, como dito no item 1 , acima, mantenha atualizado o **S.O.** de seu dispositivo.

4. Preste atenção nas últimas mudanças sociais

As mudanças sociais podem ser usadas por (ciber)criminosos para enganar as pessoas, através de várias técnicas, emails e mensagens falsas, atraindo os incautos para verdadeiras armadilhas online. Um exemplo atual são as falsas mensagens sobre o *Coronavírus* e sites falsos relacionados ao tema, que buscam induzir as pessoas a clicar em links perigosos, a abrir ou baixar arquivos maliciosos ou infectados com malwares, sob os mais diversos pretextos. Esteja atento e, em caso de dúvida, não siga as “instruções” dadas de forma maléfica ou criminosa.

5. Senhas!

Sempre crie senhas fortes para contas online. Inclua letras, números e símbolos. Senhas mais longas (pelo menos 8 ou 10 caracteres) tendem a ser mais seguras e ajudam a prevenir ataques. Não use a mesma senha para vários sites. Não use o mesmo padrão para criar senhas. Se uma senha for comprometida em um site, isso pode permitir que hackers entrem em outras contas utilizando a mesma credencial. Ou que tentem adivinhar qual foi o padrão usado na criação das senhas das diversas contas e redes que você possa usar. Não compartilhe suas senhas. Não as deixe visíveis ou anotadas. Se você está tendo problemas para lembrar todas as suas senhas, tente usar um gerenciador de senhas, como o aplicativo “KeePass” ou similares.

6. Jogos/Gamer: mantenha seu software de segurança ativado

Não desative seu software de segurança quando estiver jogando. Sim, experimentando uma conexão de alta velocidade com o mínimo de interrupções pode ser importante num jogo, mas não em detrimento da segurança. Em vez disso, procure por "modo de jogo" em seu software de segurança. Esta definição não irá interrompê-lo enquanto você está no meio do seu jogo, mas irá mantê-lo protegido.

7. Proteja-se dos softwares piratas

A melhor solução é simplesmente nunca usar sites de P2P ou similares para baixar softwares piratas. Ao invés disso, baixe seus arquivos do desenvolvedor de software original. Cuidado com o que você instala em seus computadores e dispositivos, como seu telefone celular, por exemplo. Busque desenvolvedores conhecidos e seguros. Informe-se antes de instalar um aplicativo desconhecido. Se você não tem certeza, procure ajuda, pergunte, informe-se antes.

8. Cuidado com os ataques de engenharia social

Cibercriminosos vasculham sites de mídia social o tempo todo para aprender tudo o que puderem sobre potenciais alvos. Eles vão usar as informações obtidas para enviar e-mails ou mensagens altamente elaborados, fingindo ser do seu chefe, amigo ou membro da família. Também por isso que você deve sempre observar o que diz (ou “posta”, publica) online. Revelar muita informação, como um nome do meio, nome de seus parentes, seu aniversário, onde você mora ou um nome de animal de estimação, entre tantas outras informações pessoais, pode ser o suficiente para cair nas armadilhas de criminosos cibernéticos.

9. Escolha seus amigos com cuidado (assim como na vida real, na "vida virtual")

Muitas pessoas fazem "conexões" online entre si, por meio do Facebook e de outras redes sociais. No entanto, você definitivamente estará se arriscando se não tomar o tempo necessário para filtrar quem você aceita em seu círculo de amizades virtuais. Pedidos de amizade de pessoas desconhecidas e sem a menor conexão com sua rede de amigos devem sempre ser analisados com cuidado. Além do mais, se sua conta for invadida, alguém pode espalhar "*malwares*" ***** ou mensagens do tipo "armadilha" para os computadores dos outros, em seu nome.

10. Tome cuidado ao realizar downloads (baixar arquivos, vídeos, fotos, áudios, etc.)

Tenha cuidado ao baixar anexos de e-mail (principalmente os não solicitados por você), vídeos, aplicativos, documentos, dados, etc. Eles podem uma fonte de vírus e *"malwares"* ***. Nunca instale softwares de compartilhamento de arquivos locais ao tentar visualizar um vídeo. Tenha em mente que o download de um vídeo por si só, por exemplo, nunca deve exigir que se clique um arquivo executável (.exe). O mesmo vale para outros tipos de arquivos.

11. Tenha cuidado ao usar hot spots WiFi (redes WiFi em lugares públicos e estabelecimentos diversos)

A maioria das pessoas fica empolgada ao se deparar com um local que ofereça acesso a uma rede WiFi. Mas, tome cuidado. Antes de se conectar verifique se o nome da rede é de um serviço legítimo. Uma VPN é uma boa saída, pois cria um caminho virtual protegido por senhas e criptografia, podendo garantir que seus estarão seguros e livres de ações de terceiros, mesmo se você estiver em um local público. Vários serviços estão disponíveis, mas certifique-se de usar um serviço seguro e conhecido de VPN, se for este o caso.

12. A STI/UFES não solicita dados pessoais, senhas ou qualquer informação dos seus usuários.

Qualquer e-mail ou mensagem recebida com este tipo de solicitação ou teor deve ser imediatamente excluída ou marcada como SPAM. E, certamente, nenhum dado "solicitado" deve ser informado, nenhum "formulário" preenchido, nenhuma resposta deve ser dada. Caso tenha fornecido alguma informação, recomendamos a troca IMEDIATA, por exemplo, da senha única em https://senha.ufes.br/site/alteraSenha.

Sobre as senhas de acesso às web conferencias e reuniões online (aplicações): as senhas de acesso destes aplicativos não são integradas à senha única da RedeUfes. Assim, o usuário deve acessar a ferramenta e alterar sua senha imediatamente, quando houver suspeita de acesso indevido.

*****Leia também: http://sti.ufes.br/e-mails-solicitando-dados-confidenciais

Em síntese, ficar vigilante é um bom começo, mas não é o suficiente. Não se iluda com falsas sensações de segurança. Adote boas atitudes e boas práticas de segurança online. Aprenda sempre, busque informações sólidas e atualizadas. Informe-se primeiro. Tenha cuidado com seu comportamento online. Pense: se você não iria adentrar um bairro muito perigoso à meia noite de um dia qualquer, adotando atitudes irresponsáveis quando anda por ele, por que iria se aventurar na Internet, num site perigoso ou adotar atitudes irresponsáveis nos seus dispositivos, redes e aplicativos?

06/04/2020 14:27

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

***Sobre Phishing**

Phishing é uma maneira desonesta que cibercriminosos usam para enganar e levar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos. Mensagens de Phishing parecem ser enviadas por organizações legítimas como PicPay, PayPal, Correios, uma agência do governo ou seu banco; entretanto, elas são, de fato, mensagens falsas. Os e-mails pedem, normalmente de forma educada, que você faça atualizações, validação ou confirmação de informações da sua conta, sempre dizendo que houve algum problema. Você é então redirecionado a um site falso, se enganado, e levado a apresentar informações sobre a sua conta, que podem resultar em roubos de identidade e outros prejuízos.

****Sobre Engenharia social**

Engenharia social é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Além disso, os hackers podem tentar explorar a falta de conhecimento do usuário. Graças à velocidade da tecnologia, muitos clientes e funcionários não percebem o verdadeiro valor dos dados pessoais e não sabem exatamente como proteger essas informações. Praticamente todo tipo de ataque contém algum método de engenharia social. O clássico e-mail de "phishing" e os golpes com vírus, por exemplo, são repletos de insinuações de conotação social. Os e-mails de phishing tentam convencer os usuários de que são, de fato, de fontes legítimas, na esperança de conseguir obter qualquer dado pessoal ou corporativo, por menor que seja. Os e-mails que contêm anexos cheios de vírus, por sua vez, muitas vezes alegam ser de contatos confiáveis ou oferecem conteúdo de mídia que parece inofensivo, como vídeos "divertidos" ou "fofos".

*****Sobre Malware**

O termo malware é uma contração das palavras inglesas “malicious software” (software malicioso, em tradução livre). Simplificando, malware é qualquer parte de um software que tenha sido codificada com o objetivo de danificar dispositivos, roubar dados e causar danos às pessoas. Vírus, cavalos de Tróia, spywares e ransomwares estão entre os diferentes tipos de malwares. Freqüentemente um malware é desenvolvido por times de hackers que, na maioria das vezes, estão apenas buscando uma forma de fazer dinheiro, seja pela proliferação do próprio malware ou por meio de leilão na Dark Web. De qualquer forma, pode haver outras razões para a criação de malwares. Esses softwares maliciosos podem ser usados como ferramentas de protesto, uma forma para testar a segurança de uma rede ou até mesmo como arma de guerra entre governos.