

Cartilha

Segurança da Informação para o Teletrabalho

Alerta cibernético COVID-19

Atores cibernéticos podem enviar e-mails com anexos maliciosos ou links para sites fraudulentos para induzir as vítimas a revelar informações confidenciais ou doar às causas ou instituições de caridade fraudulentas.

Tenha cuidado ao lidar com qualquer correio eletrônico com uma linha de assunto, anexo ou hiperlink relacionado ao COVID-19 e tenha cuidado com os pedidos, textos ou chamadas de mídia social relacionados ao COVID-19. Todos devem permanecer vigilantes, tomando as seguintes precauções:

- evite clicar nos links de e-mails não solicitados e tenha cuidado com os anexos de e-mail;
- use fontes confiáveis - como sites governamentais legítimos para obter informações atualizadas e baseadas em fatos sobre o COVID-19;
- não revele informações pessoais ou financeiras por e-mail e não responda a solicitações para essas informações;
- verifique a autenticidade de uma instituição de caridade antes de fazer doações;
- ao baixar aplicativos relacionados ao tema coronavírus, ainda que em lojas oficiais, é preciso ficar atento às permissões solicitadas; consulte dicas de segurança que alertam sobre os cuidados com anexos de e-mail, como evitar esquemas de engenharia social e phishing.

Cuidados ao falar sobre trabalho

- Observe onde as conversas são realizadas. Não façam chamadas em locais públicos (shoppings, cafés e espaços colaborativos).
- Os membros da equipe remota devem fazer e receber chamadas em casa ou em ambientes controlados.
- Existem pessoas mal intencionadas que circulam nesses locais afim de capturar trechos de conversa para utilizar em ataques mais sofisticados.
- limite a quantidade de dados pessoais que você está compartilhando nas mídias sociais para reduzir o cenário de ameaças;
- compartilhe informações do seu trabalho somente por meio de aplicativos em nuvem da universidade ou de companhias confiáveis.

Primeira defesa

As senhas continuam sendo a defesa da linha de frente para acessar dados e aplicativos críticos:

- Verifique se a senha do roteador doméstico não é fácil de adivinhar e não inclui seu endereço ou nome pessoal.
- Habilite a autenticação multifatorial (senha + outro requisito, como uma mensagem de texto) sempre que possível, incluindo acesso a dados críticos em aplicativos e em nuvem usados para compartilhamento de dados e documentos.
- Não use senhas fáceis como por exemplo: datas de nascimento, iniciais do nome.
- Nunca divulgar e/ou compartilhar senhas.

- Evite gravar senhas e login no computador para não facilitar roubos, principalmente se você estiver usando uma rede pública.
- Troque suas senhas periodicamente.

Seu computador pessoal é onde a maioria dos seus dados está gravada e, por meio dele, você acessa e-mails e redes sociais e realiza transações bancárias e comerciais, agora, você também o utilizará para o teletrabalho. Por isto, mantê-lo seguro é essencial para se proteger dos riscos envolvidos no uso da Internet.

Para manter seu computador pessoal seguro, é importante que você:

Mantenha softwares atualizados

Quando vulnerabilidades são descobertas, certos fabricantes costumam lançar atualizações específicas, chamadas de patches, hot fixes ou service packs. Portanto, para manter os programas instalados livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis.

Utilize softwares originais

O uso de programas não originais pode colocar em risco a segurança do seu computador já que muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciadas. Além disto, a instalação de programas deste tipo, obtidos de mídias e sites não confiáveis ou via programas de compartilhamento de arquivos, pode incluir a instalação de códigos maliciosos.

Configure mecanismos de proteção

O uso de mecanismos de proteção, como programas antimalware e firewall pessoal, pode contribuir para que seu computador não seja infectado/invadido e para que não participe de atividades maliciosas.

Seja cuidadoso ao manipular arquivos

Alguns mecanismos, como os programas antimalware, são importantes para proteger seu computador contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas e, por isto, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas. Portanto:

- seja cuidadoso ao clicar em links, independente de como foram recebidos e de quem os enviou;
- ao clicar em links curtos, procure usar complementos que possibilitem que o link de destino seja visualizado;
- não considere que mensagens vindas de conhecidos são sempre confiáveis, pois o campo de remetente pode ter sido adulterado ou elas podem ter sido enviadas de contas falsas ou invadidas.

Cuidado com locais públicos

Quando usar seu computador em público, é importante tomar cuidados para evitar que ele seja furtado ou indevidamente utilizado por outras pessoas.

Meu computador foi comprometido?

Há alguns indícios que, isoladamente ou em conjunto, podem indicar que seu computador foi comprometido. Alguns deles são:

- o computador desliga sozinho e sem motivo aparente;
- o computador fica mais lento, tanto para ligar e desligar como para executar programas;
- o acesso à Internet fica mais lento;
- o acesso ao disco se torna muito frequente (luz de hd acesa);
- janelas de pop-up aparecem de forma inesperada;
- atualizações do sistema operacional ou de sistemas de proteção não podem ser aplicadas.

Acesso indevido

Outro fator importante mesmo sendo em seu ambiente doméstico, é evitar que pessoas desautorizadas tenham acesso às informações sensíveis da sua instituição. Todos esses cuidados do local de trabalho presencial devem ser estendidos a nossa casa:

- bloquear o computador ao se ausentar do local onde está trabalhando a fim de que ninguém tenha acesso aos seus dados. Se possível, configure-o para aceitar senhas complexas;
- nunca disponibilizar logins e senhas, mesmo que para colegas de trabalho;
- nunca fotografar o ambiente de trabalho, principalmente telas de computador e documentos;
- seja cuidadoso ao usar computadores de terceiros ou potencialmente infectados, para evitar que suas senhas sejam obtidas e seus e-mails indevidamente acessados;
- desligue o Bluetooth (ou outras interfaces de comunicação, como infravermelho e wi-fi) quando não estiver usando;
- ao se desfazer do computador, apague todas as informações nele contidas e restaure as opções de fábrica.

Backups

Mídias locais

Salve os arquivos de trabalho em um dispositivo extra, como pendrives, hd's externos e cartões de memória. Nesse período de teletrabalho, é preciso reduzir os intervalos entre um backup e outro. A recomendação para esse tipo de procedimento é diária.

Em caso de um incidente de ransomware, por exemplo, a restauração dos arquivos afetados deve ser resolvida com mais facilidade, excluindo os arquivos que bloqueados substituindo pelos que estão salvos no backup.

Fazer backup na nuvem também é uma forma extremamente eficaz de garantir que os dados fiquem armazenados em um ambiente seguro. Afinal, infraestruturas de computação em nuvem possuem uma série de regras de segurança e controle de acesso para reduzir ao máximo as brechas (físicas e virtuais) de tais ambientes. Tanto a universidade, quanto as grandes empresas do ramo conseguem manter sob sua guarda arquivos de um grande número de clientes sem maiores problemas.

Internet

Cuidados ao navegar

Ao navegar na grande rede, muitas vezes estamos expostos a diversos perigos e precisamos sempre estar atentos às inúmeras investidas de atacantes para coletar nossas informações. Assim, três dicas são imprescindíveis para qualquer situação na internet.

- Cuidado ao baixar arquivos! Eles podem conter vírus, materiais impróprios ou serem ilegais. Antivírus e filtros podem ajudar a proteger.
- Nunca aceite que sites instalem programas em seu computador e não faça download de nada que você não saiba exatamente o que é e de onde vem. Cuidado em especial aos arquivos compactados (.ZIP) ou com extensão .exe ;
- Utilize redes conhecidas e evite as redes wi-fi públicas que são os pontos principais para terceiros maliciosos espionarem o tráfego da Internet e coletarem informações confidenciais.

Navegadores

Ao utilizar os navegadores, mantenha-os atualizados, com a versão mais recente e com todas as atualizações aplicadas. Deixe-o configurado para verificar automaticamente atualizações, tanto dele próprio como de complementos que estejam instalados.

- Sempre leia com atenção as mensagens mostradas no navegador. Elas podem ajudar a identificar um programa malicioso ou um site falso;
- não autorizar instalação de software de desconhecidos ou de sites estranhos;
- use o bloqueio de pop-ups em seu navegador;
- ao digitar um endereço, confirme se o que está na tela é exatamente o que procurava;

Você já deve ter reparado que no início de cada site aparece a sigla HTTP ou HTTPS. A segunda geralmente vem acompanhada do desenho de um cadeado, indicando a segurança da página visitada. Mas você sabe porque um site HTTPS é mais seguro que um HTTP?

Sigla em inglês para Protocolo de Transferência de Hipertexto. É ele quem permite que os usuários se comuniquem com servidores de sites. Apesar de ter essa função importante, o HTTP não é muito seguro. É bastante comum que terceiros entrem no caminho. Essa interceptação pode acabar em roubo de dados bastante importantes e que estão em trânsito, como senhas e números de cartões de crédito.

Por que o https é mais seguro?

Funciona da mesma forma que o HTTP, com uma camada a mais de segurança. Toda a comunicação feita entre usuário e servidor é criptografada. É como se usuário e servidor falassem em uma língua que só ambos entendem; se alguém tentar interceptar no meio do caminho, não vai conseguir decifrar as informações – ou, pelo menos, será muito difícil fazê-lo, pois elas estarão codificadas.

Quanto mais pessoas ficarem on-line, haverá um aumento de golpes on-line, engenharia social e tentativas de phishing. Hackers e criminosos certamente usarão preocupações com a disseminação de vírus e o desejo insaciável de notícias para enganar as pessoas.

- Não aceite e nem abra e-mails desconhecidos. Procure saber a origem da informação e se o responsável é de confiança ou conhecido; sempre “passe o mouse” sobre o nome do remetente do e-mail para

determinar a verdadeira origem do remetente e garantir que o nome do remetente não seja fraudulento;

- não abra anexos quando o arquivo tiver .exe ou .zip no final; utilize seu e-mail institucional apenas para fins profissionais;
- jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por e-mail. Comunique-se por telefone com a instituição que supostamente enviou o e-mail e confira o assunto;
- toda organização deve divulgar um ponto de contato para que todo funcionário entre em contato quando receber um e-mail de phishing ou um ransomware individual. Essa conscientização e comunicação informarão os funcionários sobre as táticas atuais de atores mal-intencionados. Em nosso caso, o contato fica por conta do e-mail abuse@uff.br atendimento@id.uff.br.

Ferramentas de acesso a VPN na UFF

<https://www.uff.br/?q=redobre-sua-atencao-com-seguranca-digital-no-trabalho-remoto>

Certificado digital

<https://www.uff.br/?q=servidor-crie- agora-sua-assinatura-digital-e-facilite-o-seu-dia-dia>