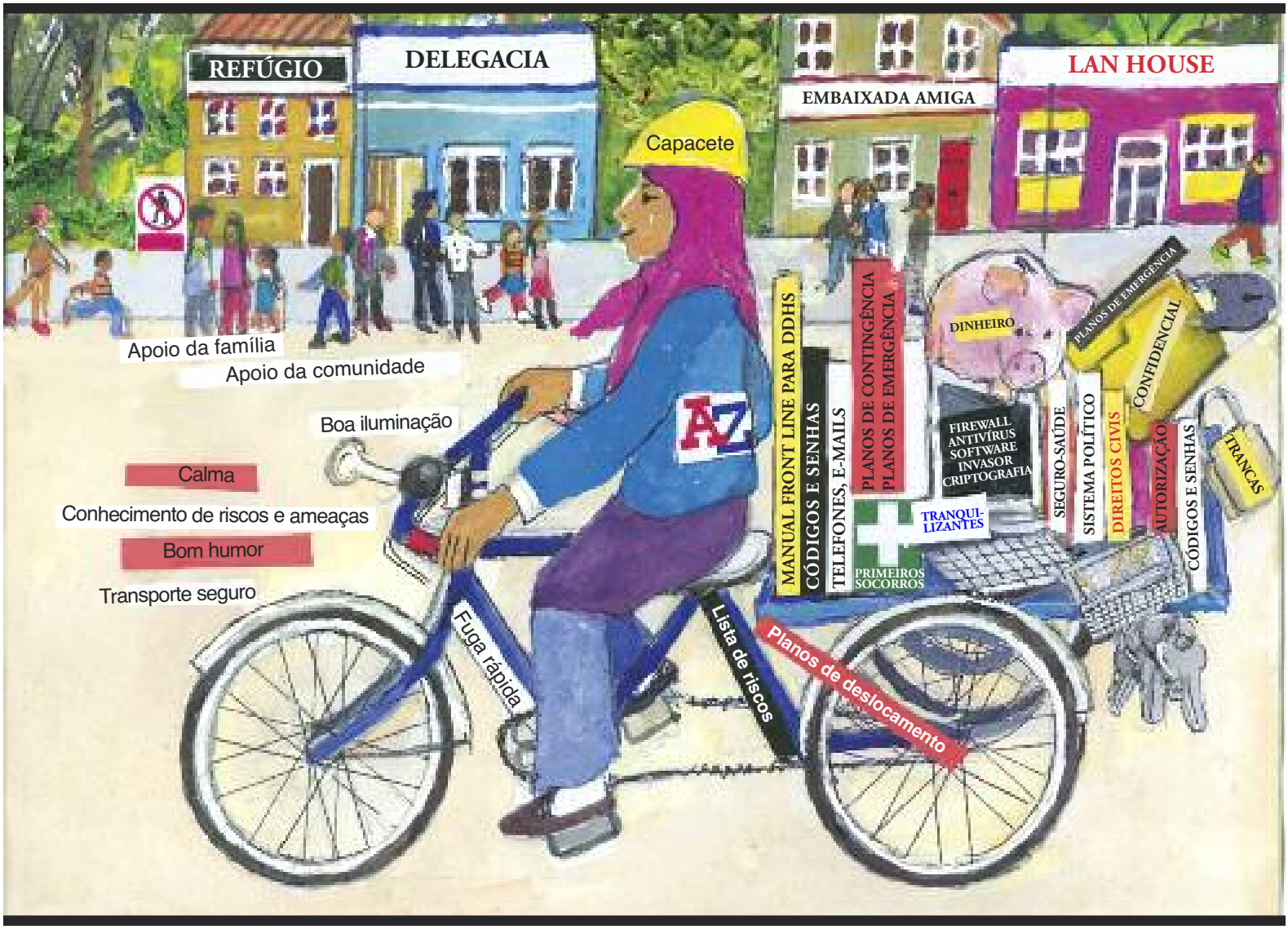
MANUAL DE SEGURANÇA:

MEDIDAS PRÁTICAS PARA DEFENSORES DOS DIREITOS HUMANOS EM RISCO



FRONT LINE DEFENDERS

ANEXO 14

Segurança no computador e no telefone

Esta lista de verificação não tem o objetivo de ser um modelo para a segurança. Seu contexto é o principal fator determinante do que deve ser verificado. Para complementar e personalizar esta lista, considere os riscos e as ameaças enfrentados por você, assim como suas vulnerabilidades. Ela é apenas uma lista dos principais pontos a ser considerados.

Para obter informações mais detalhadas, consulte Security-in-a-box (Kit de segurança digital) em https://security.ngoinabox.org

Algumas das dicas a seguir estão na seção "Awareness Cards" do projeto Security in-a-box – consulte o link acima.

1. Proteja seu computador contra hackers e softwares invasores
- Instale programas antivírus, antispyware e firewall
- Não use software pirata – usar programas ilegais aumenta sua vulnerabilidade devido à falta de atualizações e a possíveis acusações de posse de software ilegal
- Considere a possibilidade de usar software de código aberto (gratuito), como o antivírus AVAST, o antispyware Spybot e o firewall Comodor
- Use um navegador seguro como o Firefox, que tem segurança incorporada

Para obter mais informações sobre como proteger seu computador, consulte https://security.ngoinabox.org/en/chapter-1

2. Crie e mantenha senhas seguras
- Quanto mais longas as senhas, mais seguras. Suas senhas devem ter mais de 12 caracteres, letras maiúsculas e minúsculas, números, caracteres especiais e espaços, se possível.
- Suas senhas não devem conter palavras dicionarizadas nem informações sobre você disponíveis publicamente, como datas de aniversário ou nomes de amigos. Misture palavras, substitua letras por caracteres especiais ou números, misture palavras de várias línguas
- Você pode usar uma frase como senha – pode ser o título de um livro ou o trecho de uma música (substitua algumas letras por números ou caracteres especiais)
- Mude sua senha com frequência
- Defina uma senha forte diferente para cada serviço, mude as senhas com frequência e não as compartilhe. Você pode usar o KeePass para armazenar todas as suas senhas. Para obter mais informações sobre o KeePass, consulte https://security.ngoinabox.org/en/chapter-3
- NUNCA compartilhe suas senhas
- NUNCA permita que sites e programas armazenem suas senhas

Para obter mais informações sobre como proteger suas senhas, consulte https://security.ngoinabox.org/en/chapter-3

3. Como proteger arquivos confidenciais no computador
- Faça backup dos arquivos regularmente e guarde o backup num local seguro
- Oculte os arquivos confidenciais usando nomes que não identifiquem o conteúdo
- Considere a possibilidade de criptografar os arquivos, mas note que a criptografia é ilegal em alguns países e pode chamar a atenção para o conteúdo dos arquivos
- O software de código aberto (gratuito) TrueCrypt permite criptografar e ocultar arquivos
- Especialistas conseguem recuperar arquivos apagados de computadores. Use ferramentas seguras de exclusão de arquivos como o CCleaner (para limpar arquivos temporários) e o Eraser
- Se possível, verifique a reputação de seu provedor da Internet ou dos locais em que você pretende se conectar à Internet, como lan houses
- Certifique-se de que as pessoas com quem você se comunica também adotem procedimentos de segurança e privacidade. A comunicação é um processo em duas vias. Não faz sentido apenas uma das partes se preocupar com medidas de privacidade e segurança.

Para obter mais informações, consulte https://security.ngoinabox.org/en/chapter-4 e https://security.ngoinabox.org/en/chapter-6

4. Mantenha a confidencialidade de suas comunicações na Internet

- Muitas contas de e-mail na Internet não são seguras (como as do Yahoo e Hotmail) e fornecem o endereço IP do seu computador nas mensagens enviadas por você. As contas do Gmail e do Riseup são mais seguras (embora a Google já tenha cedido a pressões de governos que restringem a liberdade digital)
- O uso de lan houses expõe você ao risco de vigilância. Esteja ciente dos riscos, avaliando com quem você está em contato e quais são as informações transmitidas. Apague sua senha e o histórico do navegador do computador após usá-lo
- Use "https" em vez de "http" ao se conectar à Internet usando serviços on-line, sempre que possível, para que seu nome de usuário, sua senha e outras informações sejam transmitidas de modo seguro
- Não abra anexos de e-mails enviados por desconhecidos ou que pareçam suspeitos
- Tenha cuidado principalmente ao enviar, receber e acessar informações confidenciais na Internet
- Se possível, use um aplicativo ou serviço de proxy para ocultar sua identidade na Internet. Isso permitirá que você acesse e se comunique pela Internet usando o endereço IP de outro computador
- Os programas de troca de mensagens instantâneas (chats on-line) geralmente não são seguros, mas o Skype provavelmente é mais seguro do que os outros

Para obter mais informações, consulte https://security.ngoinabox.org/en/chapter-7
e http://security.ngoinabox.org/en/chapter-8

5. Redes sociais

- Pense cuidadosamente antes de compartilhar informações sobre você, lugares que você frequenta, seus amigos, etc.
- Peça autorização se for postar informações, documentos, fotos e localização de outras pessoas
- Use senhas seguras e mude-as regularmente
- Tenha cuidado ao acessar suas contas em redes sociais de locais com acesso público à Internet – só use esses locais se tiver certeza de que eles são confiáveis. Apague sua senha e o histórico do navegador de um computador público após usá-lo
- Leia e compreenda os contratos de licença do usuário final (EULA, End User License Agreement), termos de uso e/ou documentos sobre diretrizes de privacidade. Esses documentos podem ser alterados, por isso é importante consultá-los regularmente
- Conheça as configurações de privacidade das suas contas em redes sociais. Não confie nas configurações padrão – personalize as configurações e confira-as regularmente, porque o serviço pode fazer alterações
- Tenha cuidado ao instalar aplicativos sugeridos por redes sociais. Use esses aplicativos apenas se você confiar na origem deles, souber quais informações serão divulgadas e puder controlar o fluxo das suas informações

Para obter mais informações, consulte https://security.ngoinabox.org/en/chapter-10

6. Segurança no celular

- A tecnologia e as configurações dos aplicativos atuais de telefonia celular (como mensagens SMS e chamadas de voz) não são seguras – como é possível rastrear o local em que você está e interceptar suas comunicações, sempre considere o modo mais seguro de transmitir informações importantes
- O aparelho celular mais seguro deve ser barato e sem registro, que você paga à medida que usa e descarta após o uso
- Ative a senha ou o bloqueio do chip do celular
- Não salve informações confidenciais no celular. Se isso for necessário, codifique as informações
- Fique continuamente atento ao que acontece à sua volta ao usar o celular e evite usá-lo em situações e locais arriscados
- Apague todas as suas informações do celular antes de vendê-lo ou levá-lo para consertar
- Destrua telefones com defeito e chips antes de descartá-los
- Ao trabalhar com pessoas e organizações com quem você troca informações confidenciais, considere a possibilidade de ter telefones e chips separados para uso pessoal e profissional.

Para obter mais informações, consulte https://security.ngoinabox.org/en/chapter-9