wtsnet
EMPOWERING WITH TECHNOLOGY

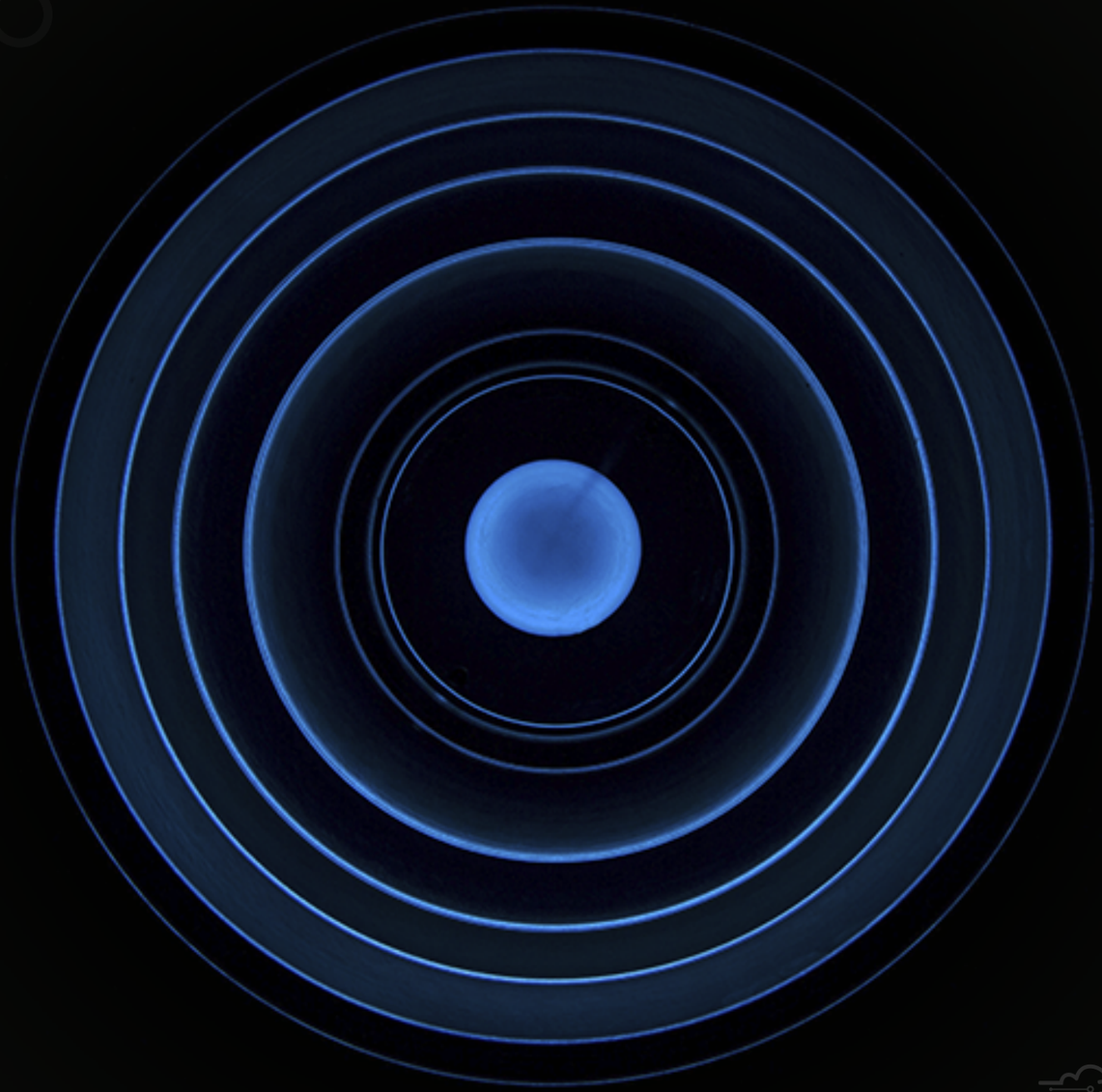
RANSOMWARE

Guia de Sobrevivência

Apesar de não serem novidades, os **ataques Ransomware** tem se tornado cada vez mais comuns afetando diversas empresas, órgãos públicos e grandes corporações.

Nos últimos anos nós da **Wtsnet atendemos dezenas de clientes com este problema e na maioria dos casos**, percebemos que se as empresas tivessem tomado algumas simples **precauções**, provavelmente o problema teria sido evitado ou amenizado.

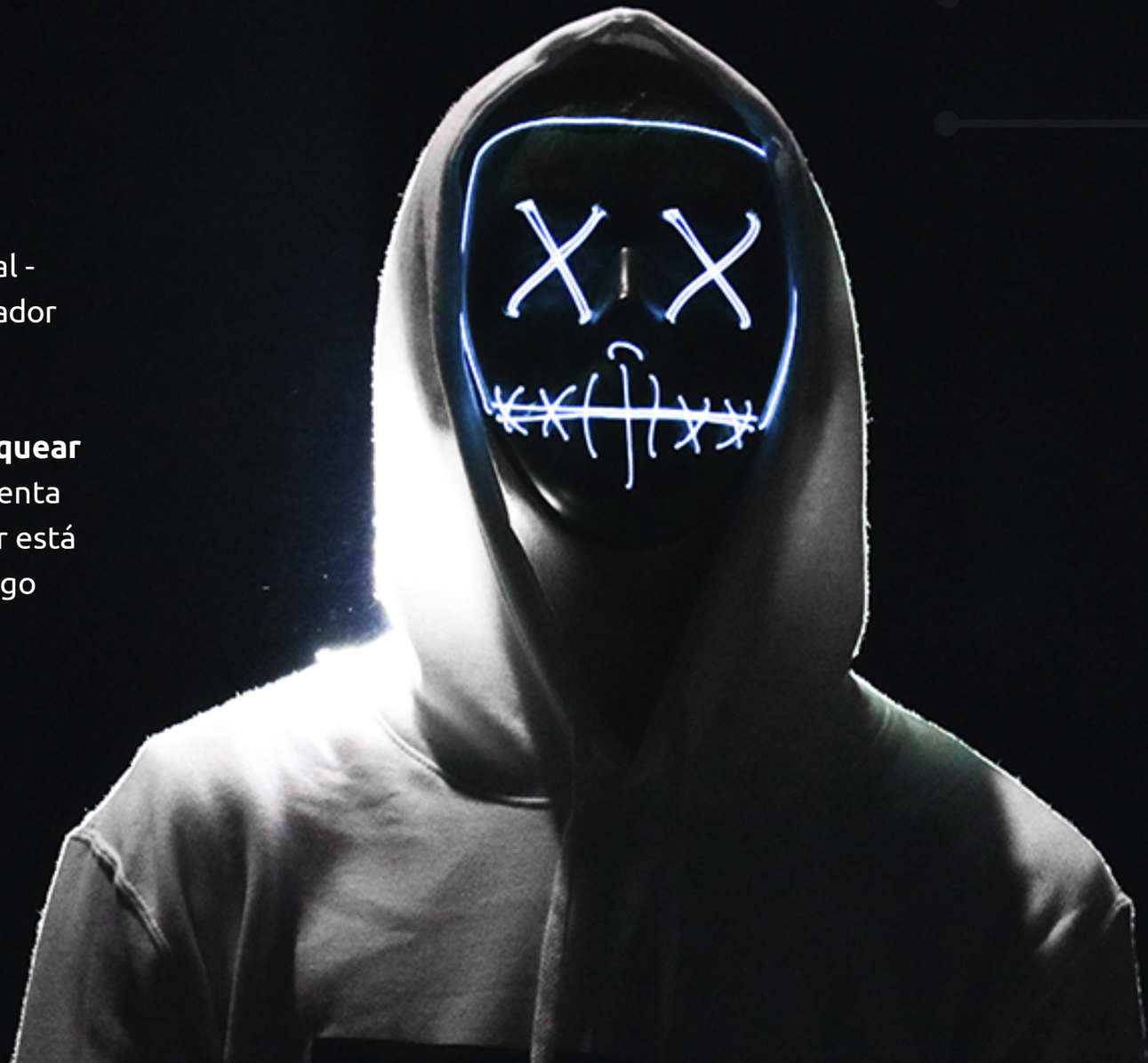
Com a intenção de que mais empresas entendam o que é o ransomware e estejam preparados para evitá-lo, criamos este E-book com algumas **dicas que serão bastante úteis para evitar o problema.**



O QUE É O RANSOMWARE?

O Ransomware é uma espécie de **malware** (software mal - intencionado) que os criminosos instalam em seu computador **sem seu consentimento**.

O Ransomware dá aos criminosos a possibilidade de **bloquear seu computador de um local remoto**. Depois, ele apresenta uma janela pop-up com um aviso de que seu computador está bloqueado e você não poderá acessá-lo, a menos seja pago um **resgate**.



COMO O RANSOMWARE FUNCIONA?

O ransomware geralmente é instalado quando você abre um anexo mal-intencionado em uma mensagem de e-mail ou quando clica em um link mal-intencionado, em e-mails, mensagens instantâneas, site de rede social ou qualquer outro website que esteja infectado, também é comum a infecção acontecer por acessos indevidos via Remote Desktop e Compartilhamento CIFS do Windows, que usam de vulnerabilidades causadas por senhas fracas para se alastrarem.

Neste tipo de ataque, os equipamentos das vítimas (sejam eles desktops, notebooks, tablets ou smartphones) são infectados por esse malware, que usa tecnologias de encriptação para **bloquear o acesso do usuário** às informações existentes naquele aparelho.

Depois que os arquivos são bloqueados e criptografados, arquivos são criados no computador da vítima **informando o sequestro das informações** e **solicitando o resgate**, também há casos em que esta comunicação é feita via e-mail.

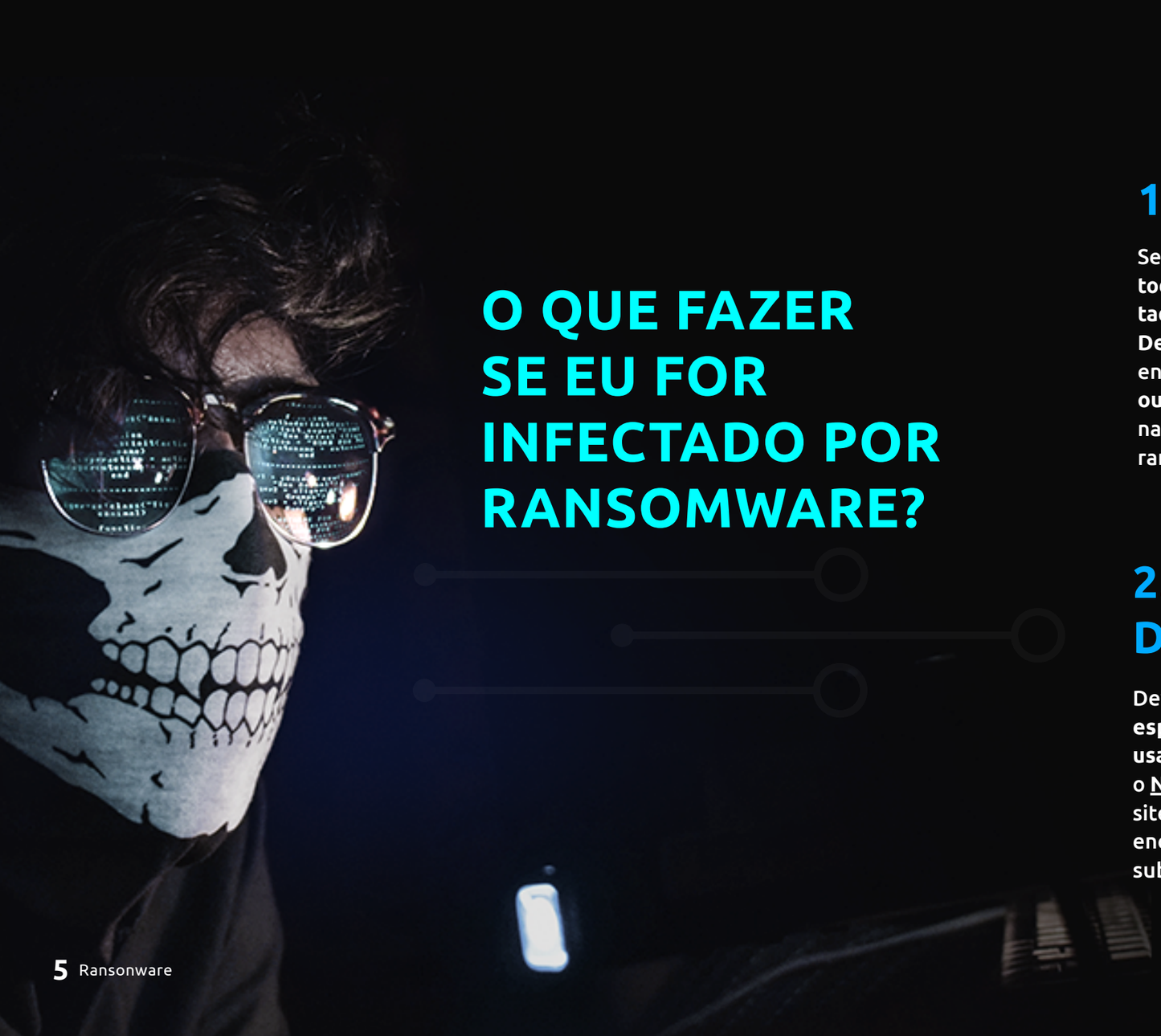
Para **liberar as informações** da máquina, o procedimento de resgate na **maioria das vezes é efetuando um pagamento em Bitcoins** – moeda virtual que dificulta o rastreamento dos valores movimentados.

Caso não pague o resgate, a vítima não terá mais acesso às informações existentes no dispositivo e, pior do que isso, poderá ter seus dados utilizados pelos bandidos da forma como bem entenderem.

Além disso, na maioria dos casos, o **equipamento fica inutilizado**, resultando também em prejuízos materiais.
Caso pague, também **não há garantias** de que o dispositivo será liberado e as informações devolvidas. Existem relatos de **vítimas que não só não tiveram seus dados devolvidos após o pagamento, como também voltaram a ser extorquidas pelos bandidos.**

Mas como proteger a rede corporativa e seus usuários desse perigo?

Agora que você já entendeu como esse malware funciona, vamos às dicas para evita-lo!



O QUE FAZER SE EU FOR INFECTADO POR RANSOMWARE?

1.MANTENHA A CALMA!

Se você contrair o ransomware, a melhor coisa a fazer é manter a calma. **Anote todas as informações possíveis** e **registre todos os arquivos sinalizados como infectados** pelo sistema operacional ou pelo software de segurança como infectados. **Desconecte-se da internet e até da rede**, pois o malware pode estar tentando enviar seus dados para os golpistas ou infectando outros computadores e **use outro PC para pesquisar detalhes do vírus**. Vírus diferentes têm diferentes vacinas, identificando o Ransomware é possível verificar se alguma empresa de segurança têm o antídoto criado.

2.IDENTIFIQUE O TIPO DO RANSOMWARE

Devido a existência de **muitas variantes**, é muito importante saber **qual delas em específico infectou** seu computador, umas das formas mais simples de fazer isso é **usar sites como o ID-Ransomware** o **NoRansom** da **Kaspersky** ou o **NomoreRansom.org** (uma iniciativa conjunta de grandes players de segurança) estes sites podem lhe ajudar respectivamente, a **identificar** a variante e até mesmo a encontrar a ferramenta para **"decriptar" os arquivos** (se você tiver sorte), bastando submeter o arquivo, e a "carta" que os cybercriminosos deixam para análise.

3.GARANTA A LIMPEZA DE SEU SISTEMA

Depois de ter identificado o tipo de ransomware que o infectou, a próxima etapa é descobrir **como removê-lo**, para isso temos algumas formas:

Forma 1 – Ferramenta de "Decriptografia"

Como dissemos acima, é possível reverter em alguns casos uma infecção de Ran somware, já citamos alguns sites que possibilitam essa ação, entretanto existem outros que podem ajudá-lo neste processo, uns mais , outros menos eficientes, abaixo segue alguns deles:

- **Kaspersky® Anti-Ransomware Tool for Busines McAfee**
- **Ransomware Recover (Mr2)**
- **Trend Micro Ransomware File Decryptor**
- **AVG Removal Tools**
- **Avast Removal Tools**

◀ **Textos clicáveis**

Algumas **soluções de Backup** como da **Acronis**, se bem implementadas, garantem proteção do Backup tanto na execução quanto em seu armazenamento. Já o restore, se torna fácil já que possível restaurar um computador ou servidor inteiro em novos equipamentos ou máquinas virtuais, sem se preocupar com drivers.

Forma 2 – Restauração de um Backup íntegro

Caso consiga remover o vírus, ótimo! Mas nem sempre isso é possível. Uma maneira de garantir a volta de sua operação com razoável rapidez é **restaurar seu backup**. Basta formatar seu computador para garantir que o vírus seja eliminado, **instalar o sistema operacional, atualizá-lo, instalar uma proteção antiransomware confiável e restaurar seus dados da mídia externa protegida** ou **de seu storage em nuvem**, esta forma inclusive tem despontado como excelente opção de armazenamento seguro.

4.REESTABELEÇA OU REVEJA SUA PROTEÇÃO

Se você conseguiu escapar, acredite, poderia não ter sido possível. Neste momento **peça um tempo aos seus gestores**, e **analise** por onde a infecção aconteceu, inclusive pois eles vão querer saber. **Senhas fracas, falta de atualizações, antivírus ou antispam antigos ou com tecnologia defasada, portas desnecessariamente abertas para web, features desativadas, firewall sem inspeção de conteúdo e pendrives infectados.**

Tudo isso pode ter sido a **causa do seu problema**, portanto reveja meticulosamente todos estes pontos, e principalmente se não tiver tempo para gerir, estudar ou manter a gestão proativa desse ambiente. **Peça Ajuda, pois o ransomware pode voltar.**

Atualmente existem tecnologias de segurança inovadoras baseadas em Machine Learning e Deep learning, estas tecnologias buscam proteger e bloquear ameaças 0 Day, ou seja ameaças recém "lançadas" cujas vacinas sequer existem, estas ferramentas podem lhe proteger bloqueando qualquer comportamento suspeito em um determinado Device. A Sophos, com sua tecnologia de Firewall e endpoint Next-Gen com EDR possibilita a execução de ações orques-tradas e sincronizadas para que o malware não se alastre na rede em caso de infecção.

5.SE NADA DER CERTO .... NEGOCIE!

Infelizmente temos que ser pragmáticos e realistas, já que muitas empresas não investem em backup, antivírus e gestão de segurança qualificada, precisamos tocar neste ponto.

Se mesmo seguindo os passos que dissemos, não tenha sido possível a remoção, você pode partir (com a consciência dos riscos) para a **última e mais perigosa ação, a negociação!** Esta opção é comumente escolhida por empresas que valorizam muito suas informações, mas só percebem isso quando são afetadas por este malware. Alguns buscam pagar o resgate apenas para reaver seus dados. Outros tentam negociar para evitar pagar a taxa de resgate exigida. Há inclusive quem busque pagar uma quantia menor, as chances de aceitação por parte dos atacantes, acabam sendo razoáveis, porque tudo que eles querem é dinheiro, ou seja acaba sendo melhor para eles obterem uma quantia pequena do que nada.

ALERTA IMPORTANTE!

Nada, absolutamente NADA garante que após a infecção seus dados não tenham sido vazados. Se sua expectativa com a desinfecção ou o pagamento de resgate tenha sido garantir que ninguém visse aquela planilha ou banco de dados com informações vitais que mantém sua empresa viva no mercado, você está equivocado.

As dicas acima servem unicamente para que você **reestabeleça sua operação.** Os dados podem estar, mesmo com todo este processo, disponíveis para o seu maior concorrente na DarkWeb, no momento em que você põe seu último servidor em operação novamente.

DICAS
PARA USUÁRIOS EVITAREM RANSOMWARES

1. FAÇA BACKUPS CONSTANTEMENTE

Uma das primeiras e mais importantes dicas é sempre fazer **backup de seus dados.** Existem inúmeras formas de fazê-lo automaticamente, para um **servidor externo** ou **mesmo opções de configurações automáticas em nuvem.** Estes serviços são essenciais e protegerão você e sua empresa não só em caso de ransomware, mas também de em caso de desastres, panes, roubos, incêndios ou catástrofes naturais.

2. MANTENHA OS DISPOSITIVOS ATUALIZADOS

A atualização de programas, softwares e aplicações são fundamentais e não existem à toa, já que uma das técnicas utilizadas pelos hackers é explorar brechas em aplicações de softwares populares, como Google Chrome, Firefox, iTunes, Adobe Reader, Adobe Flash, Java, Skype e Firefox. **Sempre que uma atualização for necessária, não hesite em faze-la**, uma vez que geralmente ela é necessária exatamente para corrigir essas vulnerabilidades.

3. UTILIZE ANTIVÍRUS E MANTENHA-O ATUALIZADO

Tenha sempre **softwares antivírus, antimalware e um firewall** que ajudem a identificar as ameaças e sempre os **configure com senha**, já que uma das ações do ransomware antes de infectar os equipamentos é desabilitar os programas de segurança. Esses softwares são capazes de **bloquear diversos malwares** e de **impedir que os usuários abram links, arquivos e sites maliciosos.**

4. FAÇA NAVEGAÇÕES SEGURAS NA WEB

Evite sites que não tenham o certificado digital SSL (Secure Socket Layer), pois desta maneira é possível ter uma ideia se a **página é real ou é algum site malicioso** que pode sem que você perceba baixar arquivos não desejáveis.

5. DESCONFIE DE ARQUIVOS ENVIADOS POR E-MAIL, APLICATIVOS E REDES SOCIAIS

Sempre desconfie antes de abrir um anexo por e-mail, aplicativo ou rede social. **Caso não conheça o remetente, evite clicar ou abrir os anexos.** Mesmo se conhecer o remetente, atente-se às **extensões do arquivo**, principalmente os ".EXE". **Muito cuidado com extensões duplicadas, como "Arquivo.PPT.EXE".**

wtsnet

EMPOWERING WITH TECHNOLOGY

A Wtsnet tem mais de 20 anos de experiência e ao longo desses anos tem ajudado diversas empresas a descobrir suas vulnerabilidades e proteger seus dados.

Clique aqui e entre em contato conosco:

www.wtsnet.com.br

contato@wtsnet.com.br

Tel.: (11) 2090-1420