Do ambiente **DOMÉSTICO** ao **CORPORATIVO**

Gustavo J R Ferreira| Novembro - 2025


O perigo não bate na porta. Ele já está no seu Wi-Fi.

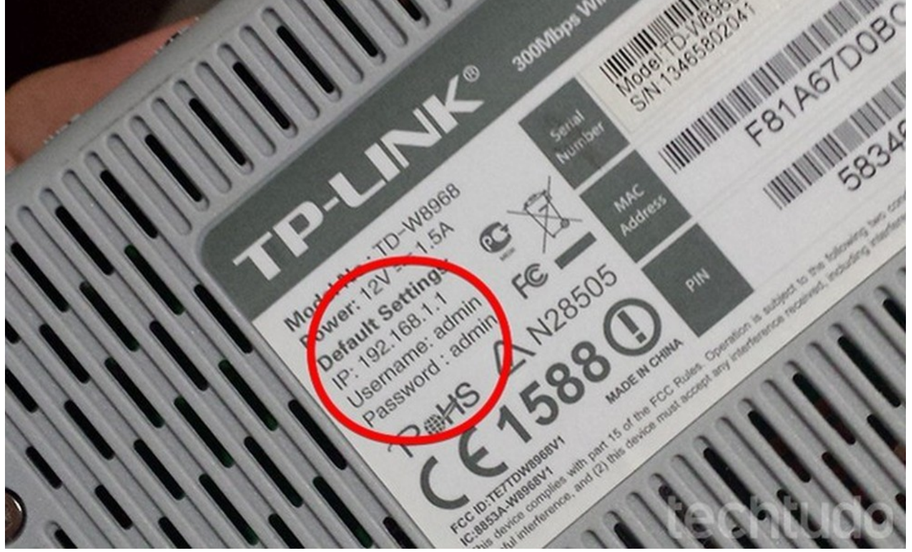
VISÃO MEET_

O SIMPLES FUNCIONA!

PESSOAS_

- 95% das violações de cibersegurança envolvem erro humano
- Phishing continua sendo o vetor de ataque mais bem-sucedido
- A maioria dos usuários reutiliza senhas em várias contas

ONDE TUDO COMEÇA_



PONTOS DE RISCO EM AMBIENTE DOMÉSTICO:

- Links Operadoras
- Uso Compartilhado
- Rede WI-FI sem proteção
- Baixo uso de recursos de segurança
- Desconhecimento sobre riscos
- Utilização de Redes Públicas: (Aeroportos - Lan Houses - Shoppings - Escolas)
- Desconhecimento dos recursos / riscos dos dispositivos móveis

meet tecnologia

MOBILE_

Os dispositivos móveis são alvos fáceis. Algumas medidas simples podem aumentar muito sua segurança.

- ✓ Atenção a mensagens de Texto – SMS; Não fornecer informações a terceiros
- ✓ Uso de senhas fortes / MFA
- ✓ Atenção as fontes de instalação de aplicativos
- ✓ Revisar periodicamente os aplicativos instalados e permissões concedidas
- ✓ Atenção a permissão de localização e rastreio de uso por outros aplicativos
- ✓ Utilizar solução de antivirus
- ✓ Habilitar criptografia no Dispositivo e Backups “Whatsapp”
- ✓ Não salvar informações sensíveis – senhas de banco e cartão em aplicativos internos
- ✓ **CUIDADO** ao utilizar autenticação facial para transações bancárias
- ✓ Evite ao máximo, ingressar o dispositivo em redes publicas, hoteis, lan-houses e aeroportos

meet tecnologia

Invasores - Nenhum Sistema Está Salvo

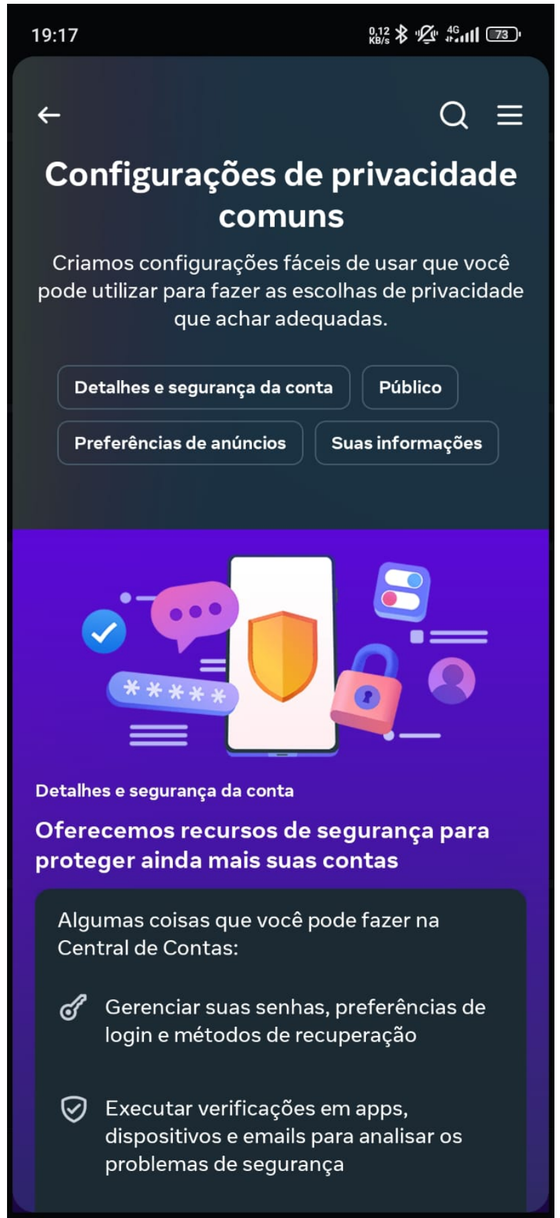
REFLEXÃO_

Tudo começa com um clique... em casa, no trabalho, na vida. E você, está preparado?

APPs_

AÇÕES SIMPLES FARÃO TODA DIFERENÇA:

- ✓ Ter curiosidade e explorar os recursos;
- ✓ Foco máximo em:
- ✓ Privacidade;
- ✓ Segurança;
- ✓ Autenticação 2FA;
- ✓ Autenticação Aplicações Externas;
- ✓ Atividades de Login;
- ✓ Controle de Dispositivos;



Instagram_

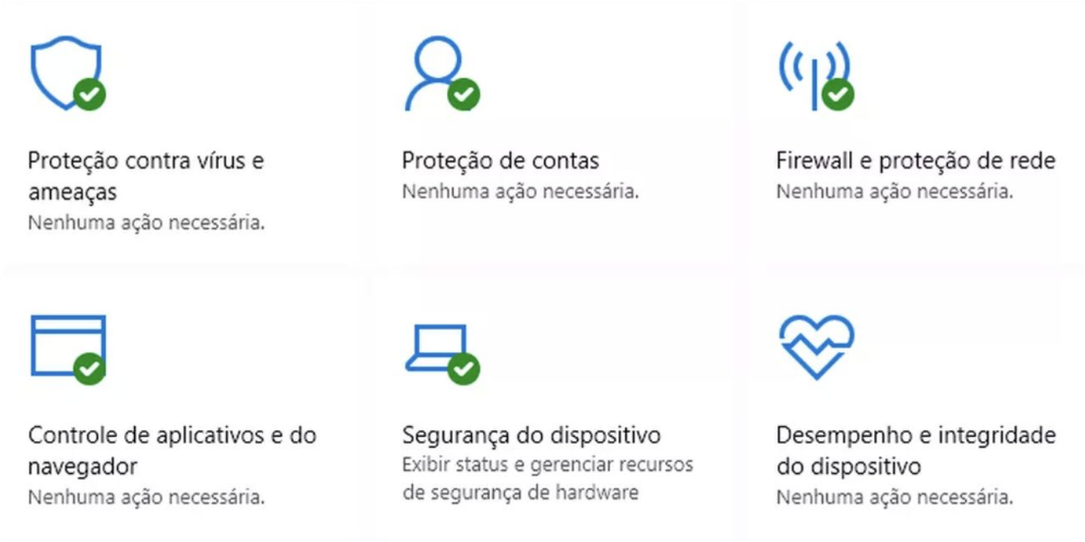
Conta Privada por Padrão:
O perfil de todos os menores de 18 anos é automaticamente configurado como privado. Isso significa que apenas os seguidores aprovados manualmente podem ver suas postagens.

Mensagens Diretas Restritas:
Adolescentes só podem receber mensagens de pessoas que eles já seguem.

Controle de Tempo de Uso:
O aplicativo envia alertas para os jovens quando atingem 60 minutos de uso diário, incentivando uma pausa.

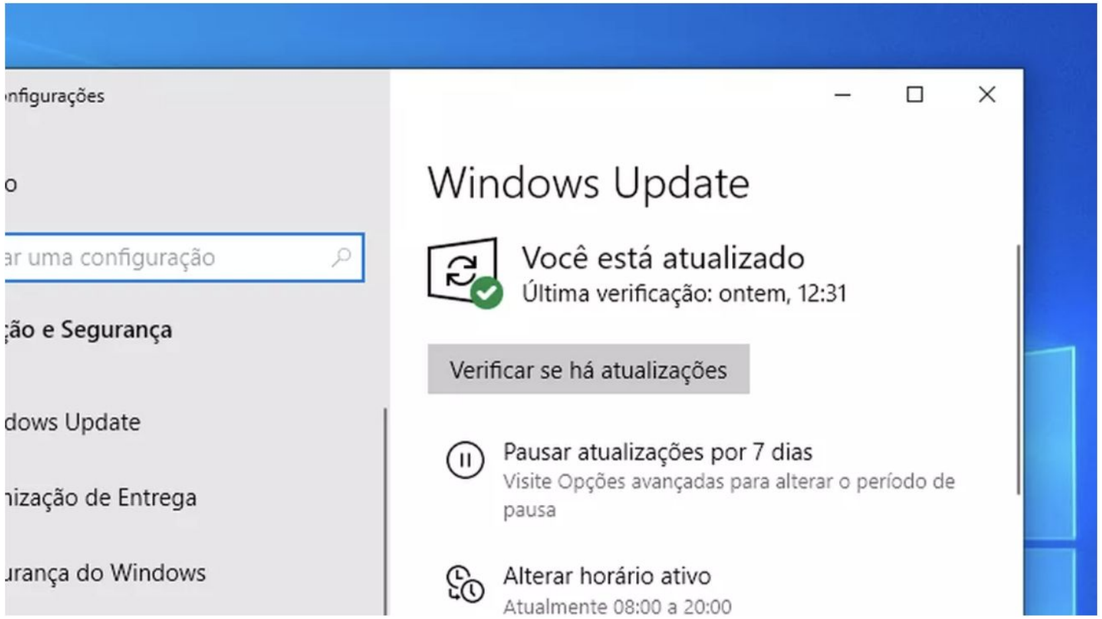
Modo Descanso Noturno:
Entre 22h e 7h, as notificações do aplicativo são silenciadas para evitar interrupções.

Windows_



AÇÕES SIMPLES FARÃO TODA DIFERENÇA:

- ✓ Ter curiosidade e explorar os recursos;
- ✓ Habilitar antivírus e Firewall do Windows
- ✓ Desligar localização e anúncios personalizados;
- ✓ Revisar perfil de redes conectados;
- ✓ Manter Windows Update sempre atualizado;
- ✓ Ativar Criptografia – Bitlocker;
- ✓ Ativar Localizador de Dispositivos;



meet tecnologia

IA’s

Gamma

deepseek

Gemini

Copilot

Deepfakes

Engano por Deepfake

•Vídeos e áudios gerados por IA agora parecem impressionantemente autênticos. Podem personificar indivíduos confiáveis com precisão assustadora.

Evolução de Golpes Personalizados

•IA analisa dados pessoais para criar golpes altamente convincentes. Ataques automatizados atingem milhões de vítimas potenciais.

Riscos em Múltiplas Camadas

•Ameaça a privacidade digital, segurança financeira e segurança física. Corrói a confiança em comunicações e fontes de mídia autênticas.

Desafios de Verificação

•Métodos tradicionais de verificação estão se tornando obsoletos. Necessidade crítica de novas tecnologias de autenticação e alfabetização digital.

CHECKLIST

- Sistema Operacional Legalizado – Windows 11;
- Windows Update Ativo e configurado para atualizações automáticas;
- Ativar a função Bitlocker no Windows;
- Sincronizar os dados da máquina no Onedrive – Quando disponível o Office 365;
- Microsoft Office 365 – Legalizado;
- Antivírus legalizado e atualizado – Bitdefender;
- Uso de senhas fortes em todos serviços, principalmente no Windows;
- Uso de MFA em todos os serviços possíveis;
- Não utilizar Pendrives ou HDs Externos compartilhados ou já utilizado em ourto dispositivo;
- Em redes desconhecidas, sempre utilizar o perfil publico;
- Evitar ao máximo utilizar redes publicas como: Hoteis – Shoppings – Aeroportos – etc.

SEGURANÇA CORPORATIVA_
Chegamos na CREDFRA

CREDFRANCO
Grupo Financeiro

Estabelece com o processo de compreensão da empresa, de suas necessidades e fragilidades!

Entendemos que Segurança da informação deve ser tratada, sempre, buscando equilibrar a produtividade esperada, à segurança necessária.

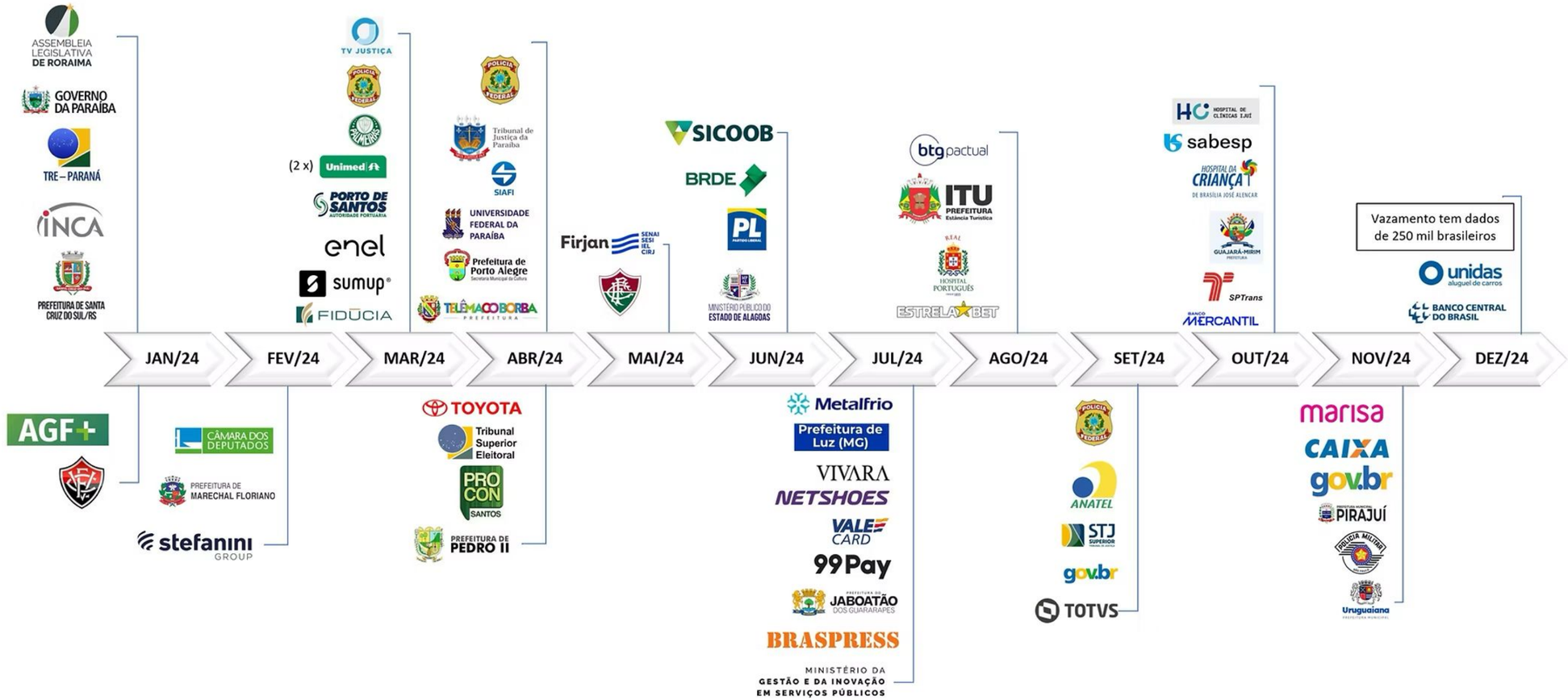
- ***Oferecer a camada de segurança necessária, mantendo a produtividade desejada do Negócio.***

Segurança é Cultura!

meet tecnologia

O motivo?

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*



- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

IBRASPD

e em **2025**....

Ataque hacker desviou R$ 710 milhões, diz empresa que opera sistema PIX

Breve análise

Lojas Renner

Alvos

Site e aplicativo das Lojas Renner

Impactos mensuráveis

+ R$525 Mi

de perda de valor de mercado

+ R$15 Mi

de perda de faturamento diário

Impactos imensuráveis

- Imagem da empresa;
- Perda de dados;
- Atrasos na entrega de produtos
- Redução de produtividade;

https://bipbrasil.com.br/a-escalada-de-ataques-ciberneticos-em-varejo-e-bens-de-consumo-e-como-se-proteger/

PILARES FUNDAMENTAIS

Como em todo o processo de construção, nos norteamos em **4 pilares** para construção do **ambiente adequado** e desejado.

Políticas
- PSI
- Política Senhas
- P.Gestão Ativos

Processos
- POPs
- Integração entre setores
- Contratação / Admissão/ Demissão
- Auditorias

Tecnologia
- Sistemas
- Monitoramento
- Anti-Malware
- Backups

Pessoas
- Conscientização
- Treinamento
- Termos

meet tecnologia

TECNOLOGIAS_

SOLUÇÕES:

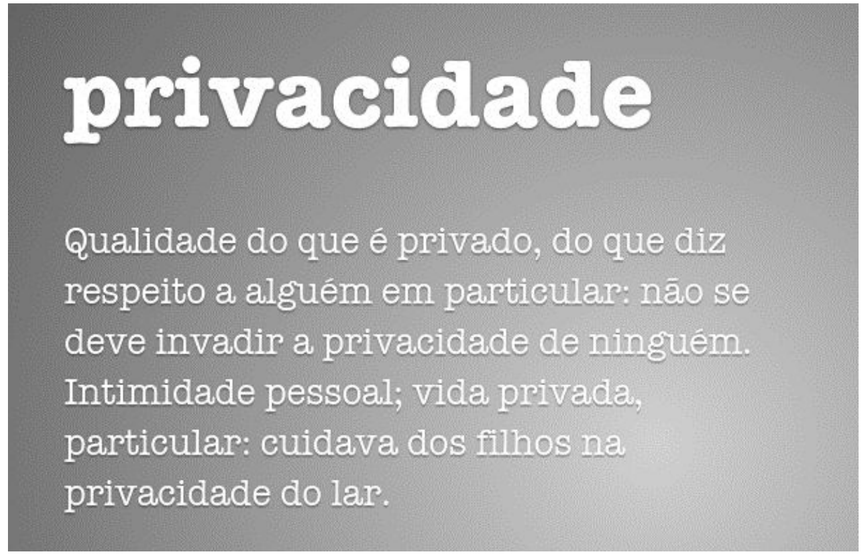
- Antivírus
- Antispam
- Firewall
- IDS & IPS
- Controle de Patchs - Atualizações
- SIEM
- Gestão de Vulnerabilidades
- Gerenciamento de Senhas - Credenciais
- Acessos Seguros
- Criptografia
- Bloqueio por GEOIP

meet tecnologia

PRIVACIDADE_

PRIVACIDADE, NOS DIAS DE HOJE, AINDA EXISTE?

A privacidade é um direito, mas todos precisam fazer sua parte para mantê-la.



LICENCIAMENTO DE SOFTWARE_

Diferentemente de épocas passadas, quando softwares piratas eram comuns nas empresas, hoje essa prática é considerada "trazer problemas para sua casa".

Instalação de Crack

Usar "cracks" ou ativadores introduz código imprevisível em seu sistema.

Comprometimento de Segurança

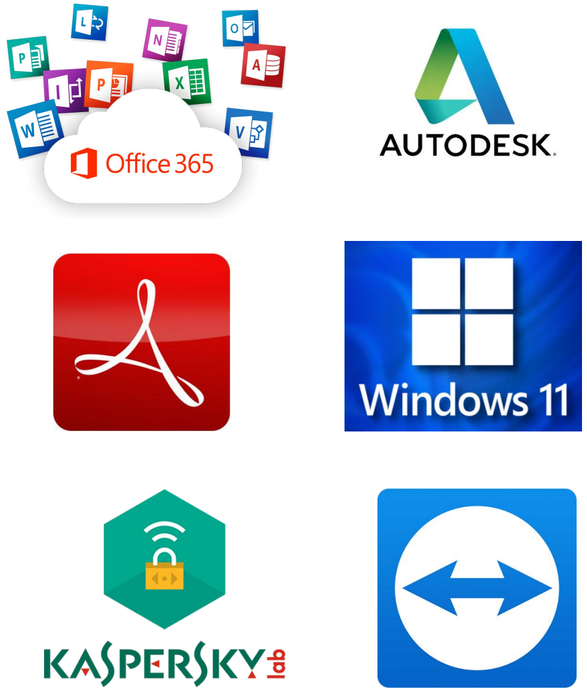
Essas ferramentas podem contornar estruturas de segurança cuidadosamente planejadas instantaneamente.

Invasão de Privacidade

Impossível garantir que essas ferramentas não estejam monitorando sua atividade.

Portal para Malware

Frequentemente contém programas ocultos que comprometem a integridade do sistema.



O "benefício" financeiro de curto prazo cria vulnerabilidades de longo prazo que nenhum sistema de segurança pode mitigar completamente.

BOLETOS FALSOS_

Fonte: https://www.kaspersky.com.br/ - https://portal.febraban.org.br/noticia/3391/pt-br/

Dinheiro não está sobrando e sair distribuindo por aí — e por engano — não é nada divertido. Você já deve ter ouvido relatos sobre o “golpe do boleto falso”, em que uma pessoa que realmente fez uma compra ou tem uma conta em aberto recebeu um boleto de forma digital ou impressa e, quando pagou, o dinheiro não quitou a dívida e foi para outro lugar.

Sugestões:

- ✔ Sempre confira os dados do beneficiário
- ✔ Não imprima os boletos
- ✔ Confira os dados do banco emissor
- ✔ Sempre que possível use o DDA
- ✔ Desconfie de código de barras falhando

RANSOMWARE_

O **ransomware** representa uma ameaça para você e seu dispositivo, mas o que torna essa **forma de malware** tão especial? A palavra \"ransom\" (resgate) já diz tudo sobre essa praga. **Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo**.

Na maioria dos casos, a infecção por ransomware ocorre da seguinte maneira:

1. O malware primeiro ganha acesso ao dispositivo
2. Dependendo do tipo de ransomware, todo o sistema operacional ou apenas arquivos individuais são criptografados
3. Um resgate é, então, exigido das vítimas em questão.

Fonte: https://www.kaspersky.com.br/

LGPD

Lei Geral de Proteção de Dados Pessoais

A **Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018**, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

Conclusões_

		
Comece em Casa Bons hábitos de segurança começam na vida pessoal	**O Simples Funciona** Práticas básicas e consistentes geralmente são melhores	**Mantenha-se Atento** Educação é sua defesa mais forte

NÃO SE ESQUEÇA!

Obrigado.

meet tecnologia

SUPREMA PROXYS_ mgcloud

Instagram

Linkedin