CHECKLIST PREMIUM
Blindagem de Identidade Digital

O passo a passo definitivo para proteger seus dados em 2026.

Sua identidade digital vale ouro. E os cibercriminosos sabem disso. Este documento não é apenas um texto; é um plano de ação tático. Ao preencher cada caixa abaixo, você estará construindo uma muralha intransponível ao redor das suas informações financeiras, e-mails e redes sociais.

Imprima este guia ou marque digitalmente. **O importante é agir agora.**

FASE 1: Auditoria e Diagnóstico de Risco

Antes de construir muros, precisamos saber se alguém já invadiu a sua casa. Esta fase garante que você não tem portas abertas esquecidas.

☐ **Varredura de E-mail:** Acesse o site *Have I Been Pwned* (haveibeenpwned.com).

☐ **Checagem de Resultados:** Digite seu e-mail principal. A tela ficou vermelha? Anote quais serviços foram vazados.

☐ **Troca Imediata:** Acesse os serviços comprometidos indicados na varredura e troque a senha imediatamente.

☐ **Exclusão de Contas Fantasmas:** Apague contas antigas de fóruns, lojas ou redes sociais que você não utiliza há mais de um ano.

FASE 2: O Cofre de Alta Segurança

Esquecer senhas ou usar a mesma palavra para tudo é o erro fatal número um. A partir de hoje, você só precisará decorar **uma única senha**.

☐ **Escolha o Cofre:** Baixe um gerenciador de senhas confiável (Recomendação de Elite: *Bitwarden* ou *1Password*).

☐ **Crie a Senha Mestra (Master Password):** Invente uma frase longa, sem sentido lógico, mas fácil de lembrar (Exemplo: *GatoAzul$PulaMuro1999!*).

☐ **Geração Aleatória:** Use o cofre para gerar senhas de pelo menos 16 caracteres (com letras, números e símbolos) para o seu e-mail principal e banco.

☐ **Nunca Salve no Navegador:** Desative a opção do Chrome/Edge/Safari de salvar suas senhas. Elas são alvos fáceis para malwares locais.

FASE 3: A Barreira Intransponível (MFA)

A Autenticação de Dois Fatores (MFA / 2FA) é o que impede um hacker de acessar sua conta, mesmo que ele tenha descoberto a sua senha.

☐ **Abandone o SMS:** O envio de código por SMS é vulnerável a ataques de *SIM Swap* (clonagem de chip). Pare de usar.

☐ **Baixe um Autenticador:** Instale o *Authy*, *Google Authenticator* ou o próprio autenticador do seu cofre (Bitwarden).

☐ **Blinde o E-mail Base:** Ative o 2FA via aplicativo no seu e-mail principal (Gmail, Outlook). Ele é a chave para recuperar todas as outras contas.

☐ **Blinde Finanças e Redes:** Ative o 2FA via aplicativo no seu banco, WhatsApp, Instagram e LinkedIn.

FASE 4: Comportamento de Elite

A melhor tecnologia do mundo não supera o erro humano. Ajuste seus hábitos diários com este protocolo final.

☐ **Regra do Wi-Fi Público:** Nunca acesse contas bancárias ou e-mails usando o Wi-Fi gratuito de shoppings, cafés ou aeroportos sem uma VPN ativa.

☐ **Atenção ao Phishing (Engenharia Social):** Bancos nunca pedem sua senha por SMS ou e-mail. Na dúvida, abra o aplicativo oficial diretamente.

☐ **Atualização Silenciosa:** Ative a atualização automática no seu celular (iOS/Android) e no seu computador (Windows/macOS). Hackers exploram brechas antigas.

☐ **Agendamento Trimestral:** Coloque um alerta no calendário para daqui a 90 dias: ”Refazer a Auditoria de Segurança (Fase 1)”.

Você acaba de eliminar 99% das suas chances de sofrer um golpe digital.
Mantenha-se seguro. Mantenha-se no controle.