A NAVEGAÇÃO SEGURA NA REDE

é a proteção de todos no presencial e no teletrabalho

SUMÁRIO

SENHAS

Vamos aprimorar a navegação segura no acesso à rede interna?

- **Sistemas precisam identificar os usuários;**
- **Senha é a forma mais básica, mas existem outras;**
- **Senhas mais comuns: 123456, 1234, 102030, password, master, qwerty, 111111;**

FIQUE DE OLHO NA ORIENTAÇÃO.

A sua senha de login de rede deve ser trocada a cada
60 dias.

Para isso, se liga nas dicas:

- **Não repita as últimas cinco senhas já utilizadas;**
- **Não use palavras do próprio nome, nem do(a) filho(a), pais, cônjuges;**
- **Evite também a usar dados pessoais (aniversário, placa do carro) ou do seu interesse (cantor favorito, personagens de livro);**
- **Jamais utilize as sequências óbvias de números (123456789) e do alfabeto (abcdefghij);**
- **Evite reutilizar a mesma senha em mais de um sistema;**
- **Senhas vazadas são testadas em diversos sistemas;**
- **Para criar a sua senha forte, utilize no mínimo 10 caracteres. É isso mesmo, dez caracteres;**
- **Está liberado o uso mesclados de letras maiúsculas e minúsculas, números e caracteres especiais.**

MUITO IMPORTANTE!
Sua senha é uso pessoal e intransferível

TELETRABALHO

No teletrabalho, é importante fortalecer a segurança de navegação na rede.

A autenticação multifator é mais um nível de proteção para o acesso ao seu login da conta institucional.

Desde de 11 de abril de 2023, deve ser utilizado o aplicativo Microsoft Authenticator para configurar a autenticação multifator.

Na loja de aplicativos de seu dispositivo móvel, baixe e instale o aplicativo Microsoft Authenticator e configure sua conta institucional.

Orientações adicionais:
https://sway.office.com/VcreE2HPQG7I8gDw?ref=Link

Dúvidas pela Central de Serviços:
https://centralservicos.tjpa.jus.br/glpi/

E-MAIL

Não caia nas armadilhas enviadas por e-mail.

O e-mail institucional é o seu instrumento de comunicação com as unidades administrativas e judiciárias. Por isso, deve ser utilizado para o contato corporativo.

Evite o uso do e-mail institucional para assuntos pessoais nem para cadastro em site de compras on-line. Sua conta de e-mail institucional pode se tornar porta de entrada para invasores, se cair em mãos erradas.

Armadilhas mais comuns em e-mail são o spam e o phishing.

Você sabe a diferença? Vamos lá!

- **O phishing é aquele e-mail de conteúdo duvidoso para obter ilegalmente dados pessoais por meio de um link ou um "clique aqui"**
- **O spam pode ocorrer por e-mail enviado para um grande número de usuários com conteúdo indesejado. O remetente pode ser conhecido ou não. Mesmo assim, é bom ficar em alerta.**

E-mails com remetentes externos à Instituição e desconhecidos devem ser verificados de forma cuidadosa. E-mails estranhos podem ser indicativo de ataques cibernéticos.

TODO CUIDADO É POUCO!

- Ao receber um e-mail suspeito, não clique no link disponível. Pode conter arquivo malicioso e contaminar o seu computador e a rede.
- Não faça download do anexo de mensagens inesperadas.
- Nada de responder ao remetente desconhecido ou que não tenha o hábito de se comunicar.
- Fique de olho se a mensagem tiver o tom assustador, inusitado ou extraordinário ou de promoção/oferta mirabolante.
- E-mail com desvio linguístico da língua portuguesa é um sinal de alerta.
- Prefira digitar a URL, o site ou o endereço eletrônico a clicar diretamente no link.
- Jamais responda e-mail inusitado ou desconhecido com dados confidencial ou pessoal.
- Fique alerta, tome cuidado e procure por algum indício de que seja uma isca.

DISPOSITOS EXTERNOS
(PEN-DRIVE, HD, CARTÃO DE MEMÓRIA)

Manter o seu computador e rede em segurança evita malwares e vírus com tentativa de ataques cibernéticos.

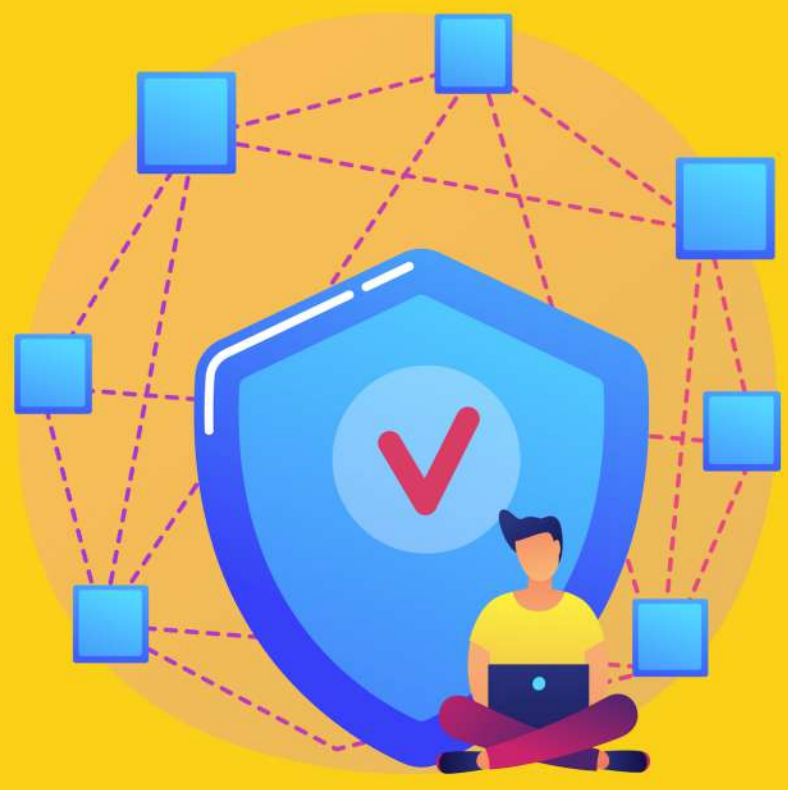
Malware é todo software (programa) malicioso que foi projetado para provocar prejuízo, seja explorando o computador e a rede ou ainda na tentativa de furto de dados confidencial ou pessoal.

Aparentemente inofensivos, os dispositivos externos, como pen-drive, HD externo e cartão de memória, podem guardar malware e vírus, já que foram utilizados em mais de um computador.

Evite o uso de dispositivos externos em seu computador de trabalho. Isso protege a rede de invasão por malware e vírus, evitando a infecção.

Canal de contato para dúvidas/reclamações/sugestões relacionadas à segurança da informação:

seginfo@tjpa.jus.br



PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
GESTÃO BIÊNIO 2023-2025

PRESIDENTE
DESA. MARIA DE NAZARÉ SILVA GOUVEIA DOS SANTOS
VICE-PRESIDENTE
DES. ROBERTO GONÇALVES DE MOURA
CORREGEDORIA GERAL DE JUSTIÇA
DES. JOSÉ ROBERTO PINHEIRO MAIA BEZERRA JÚNIOR

COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL DE JUSTIÇA DO PARÁ

DESA. LUZIA NADJA GUIMARÃES NASCIMENTO
Presidente do Comitê
JUIZ AUXILIAR DA PRESIDÊNCIA SÍLVIO CESAR DOS SANTOS MARIA
Coordenador do Comitê
PATRÍCIA CASSEB
Secretária do Comitê
MÁRCIO GÓES DO NASCIMENTO
Secretário de Informática
MIGUEL LUCIVALDO ALVES SANTOS
Secretário de Planejamento, Coordenação e Finanças
VICENTE DE PAULA BARBOSA MARQUES JUNIOR
Secretário de Administração
CAMILA AMADO SOARES
Secretária de Gestão de Pessoas
TIAGO SILVA GUIMARÃES
Secretário de Auditoria Interna
CRISTHIANNE DE CAMPOS CORREA
Secretária-Geral da Escola Judicial
ERICK JOHN MACIEL BOL
Coordenador de Suporte Técnico
WILL MONTENEGRO TEIXEIRA
Diretor do Departamento de Comunicação
FÁBIO DJAN OLIVEIRA DE LIMA
Diretor do Departamento de Planejamento, Gestão e Estatística

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ

1874

NON SIBI SEMPER FIDELIS AD JUSTITIA

150 1874 | 2024 TJPA

Gestão 2023-2025

Novos passos, novas caminhadas.