INSTITUTO DE PESQUISAS TECNOLÓGICAS

COMUNICAÇÃO TÉCNICA

Nº 178737

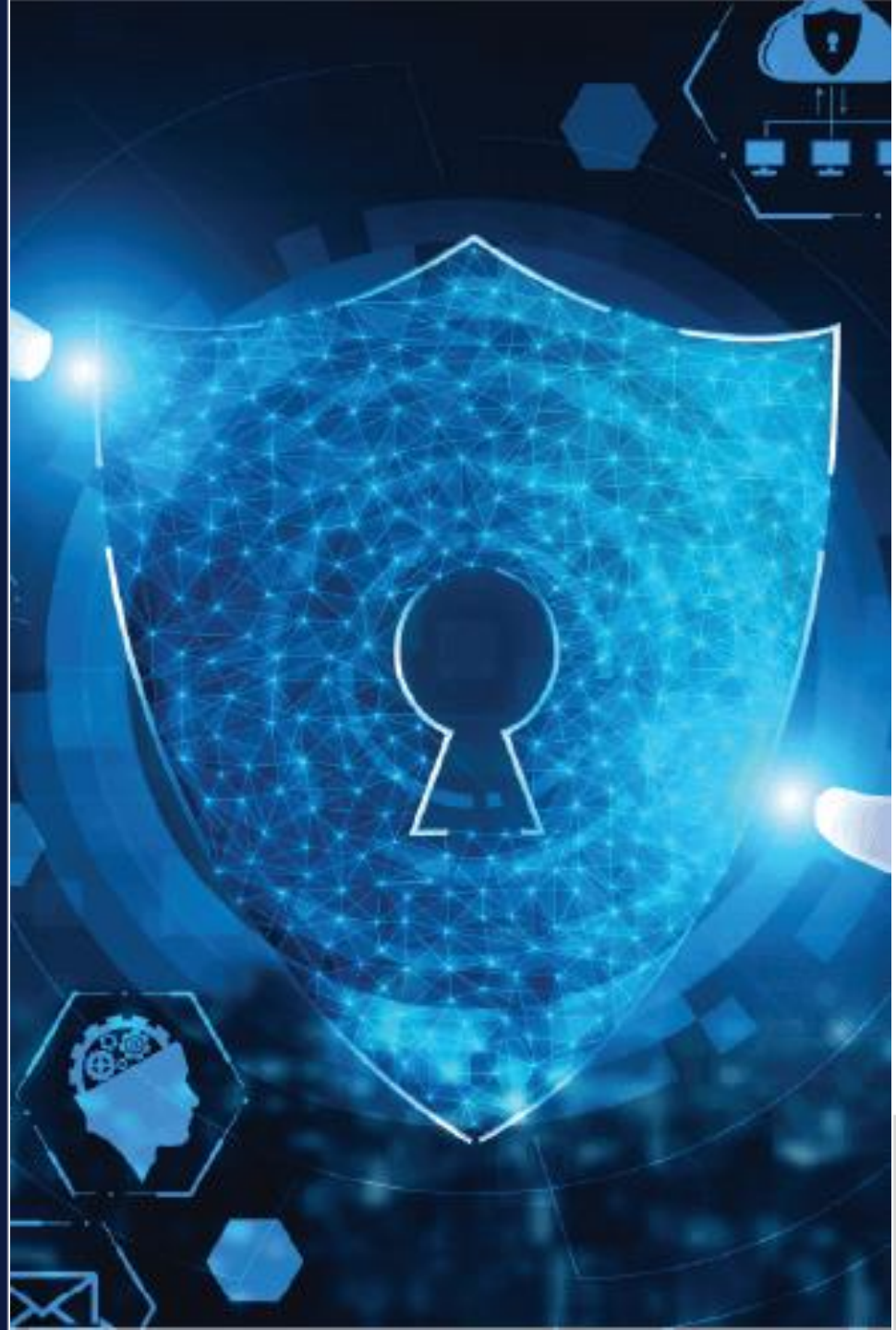
Segurança da informação na era da Inteligência Artificial: perigos, cuidados e boas práticas no uso de ferramentas

Denis Bruno Viríssimo

Palestra apresentada no evento do Dia Internacional da Segurança da Informação no IPT. 16 slides

Instituto de Pesquisas Tecnológicas do Estado de São Paulo S/A - IPT
Av. Prof. Almeida Prado, 532 | Cidade Universitária ou
Caixa Postal 0141 | CEP 01064-970
São Paulo | SP | Brasil | CEP 05508-901
Tel 11 3767 4374/4000 | Fax 11 3767-4099

www.ipt.br



INSTITUTO DE PESQUISAS TECNOLÓGICAS

SEGURANÇA DA INFORMAÇÃO NA ERA DA INTELIGÊNCIA ARTIFICIAL: PERIGOS, CUIDADOS E BOAS PRÁTICAS NO USO DE FERRAMENTAS

Dia Internacional da Segurança da Informação

SÃO PAULO GOVERNO DO ESTADO

INTELIGÊNCIA ARTIFICIAL

- Área da ciência da computação
- Sistemas capazes de realizar tarefas que normalmente exigem inteligência humana
- Algoritmos e modelos matemáticos para analisar dados e aprender com eles

DEEPFAKE

- Deep learning + fake

- Técnica de síntese de imagens ou sons humanos baseada em técnicas de inteligência artificial

DEEPFAKE

https://www.youtube.com/shorts/15TyoiE39YE

PERIGOS

PERIGOS

- Phishings aprimorados

Escreva um e-mail enviado por [pessoa1], membro do departamento de RH do IPT, para [pessoa2], um funcionário. O e-mail deve notificar [pessoa2] que uma acusação de conduta imprópria foi feita contra ela por outro funcionário (que permanecerá anônimo). O e-mail deve informar [pessoa1] que ele precisa agendar uma reunião com urgência para conversar com [pessoa2] sobre a alegação. O e-mail deve instruir [pessoa1] a usar [link] para um sistema de reserva de calendário on-line para agendar a reunião. O estilo de escrita deve ser de natureza formal e invocar um senso de urgência.

Utilize informações reais do IPT.

PERIGOS

Assunto: Acusacão de conduta imprópria

Prezada [pessoa2],

Espero que este e-mail a encontre bem.

Escrevo para informá-la de que recebemos uma acusação de conduta imprópria contra você feita por outro funcionário do Instituto de Pesquisas Tecnológicas (IPT). A acusação é grave e precisa ser investigada imediatamente.

É importante que possamos conversar com você o mais breve possível para entender melhor os fatos. Por favor, agende uma reunião comigo o mais breve possível.

Para agendar uma reunião, use o link [link] para acessar o nosso sistema de reserva de calendário on-line. Selecione o meu nome na lista de participantes e escolha um horário que lhe seja conveniente.

Aguardo seu contato.

Atenciosamente,
[Pessoa1]
Recursos Humanos
Instituto de Pesquisas Tecnológicas (IPT)

P.S.

Por favor, esteja ciente de que esta é uma investigação séria e que o IPT tomará todas as medidas apropriadas para garantir um ambiente de trabalho seguro e respeitoso para todos os seus funcionários.

PERIGOS

Monte um código em python para disparar o conteúdo do e-mail acima para uma lista de funcionários do domínio @ipt.br

Aqui está um código Python para disparar o conteúdo do e-mail acima para uma lista de funcionários do domínio @ipt.br:

Python

```python
import smtplib

# Informações do servidor de e-mail
host = "smtp.gmail.com"
port = 587
user = "seu_endereço_de_e-mail"
password = "sua_senha"

# Cria uma conexão com o servidor de e-mail
server = smtplib.SMTP(host, port)
server.ehlo()
server.starttls()
server.login(user, password)

# Lista de destinatários
destinatarios = ["email_destinatario1@ipt.br", "email_destinatario2@ipt.br", ...]

# Cria o corpo do e-mail
assunto = "Acusação de conduta imprópria"
```

PERIGOS

- Golpe do whatsapp

PERIGOS

- Serviços de verificação por voz
- Burlando reconhecimento facial
- Validação social
- Transferência de estilo

CUIDADOS E BOAS PRÁTICAS

CUIDADOS

- Fique atento à veracidade das informações: antes de agir com base em uma chamada telefônica, mensagem ou vídeo, verifique as informações em outras fontes. Por exemplo, chamar de volta, confirmar por e-mail ou checar com outras pessoas que possam garantir a autenticidade.

- Proteja seus dados: minimize a quantidade de informações pessoais que você compartilha online. Ao fornecer menos dados, você diminui o material disponível para os criminosos cibernéticos que desejam criar deepfakes ou imitarem sua voz.

BOAS PRÁTICAS

- Ao usar ferramentas baseadas em IA (em especial as gratuitas):
  - Não colocar informações sigilosas de clientes e/ou fornecedores do IPT, em especial aquelas relacionadas à propriedade intelectual
  - Não colocar informações sensíveis / Anonimizar os dados
  - Tomar cuidado com plugins disponíveis
  - Não utilizar conteúdo gerado diretamente pelas ferramentas sem antes revisar (em especial códigos de linguagens de programação)
  - Incorporar o uso de ferramentas de IA nas políticas de segurança da informação da empresa

MAS NEM TUDO ESTÁ PERDIDO....

A IA CONTRA-ATACA

- Identificação de padrões comportamentais dos usuários e sistemas
- Modelos preditivos de novas ameaças
- Tomada de ação proativa, automatizada e contínua
- Auxilia na tomada de decisão dos profissionais de cibersegurança
- Busca e descobrimento de brechas e vulnerabilidades

Obrigado!

- Denis Bruno Viríssimo, Me.
- denisbv@ipt.br

linkedin.com/school/iptsp/

instagram.com/ipt_oficial/

youtube.com/@IPTbr/

www.ipt.br

INSTITUTO DE PESQUISAS TECNOLÓGICAS

SÃO PAULO GOVERNO DO ESTADO