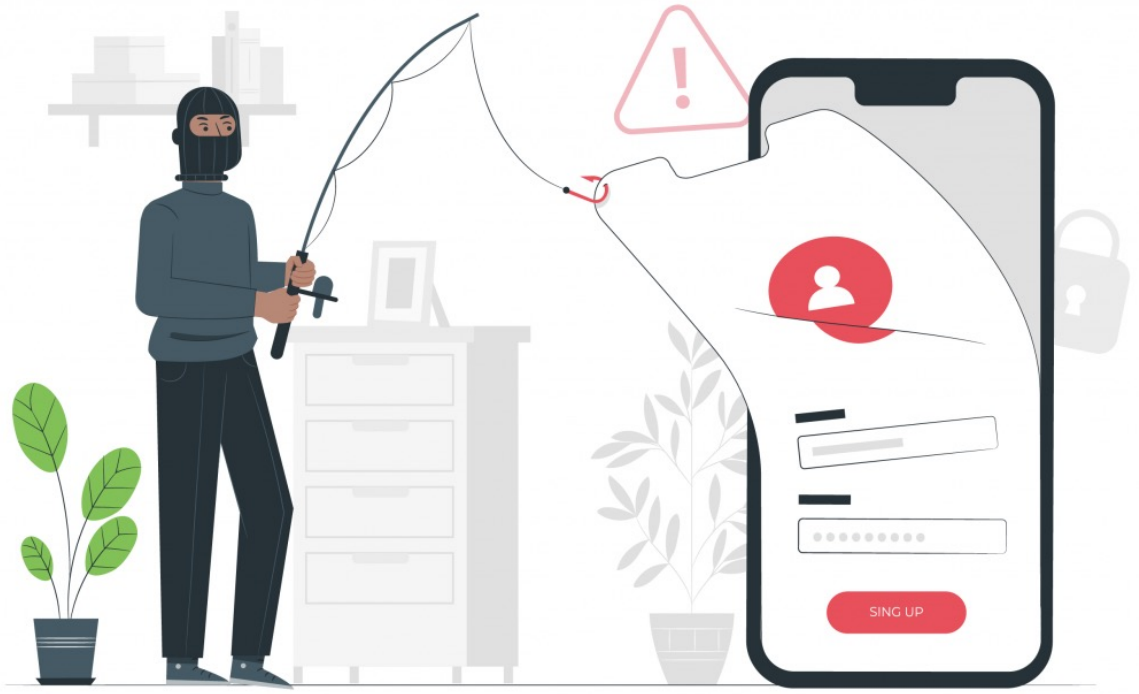

hackone
NSE1: MAUS ATORES
NOME DO MENTOR: ALEXANDRE SABINO

PHISHING

- E-mail especialmente criado que parece ter sido enviado pelo sistema real
- Link Falso
- Atacantes motivados por indignação política, social ou moral



DDOS – ATAQUE DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO

- **Servidor de Comando e Controle (C&C)**
- **BOTNET**
- **Intimidar seus inimigos causando transtornos, caos e danos**

CIBERTERRORISTAS

- **Grupo bem financiado**
- **Muita engenhosidade para atacar pessoas de alto perfil**
- **Utilizam ataques DDoS**
- **Se infiltram em sistemas para roubar dados pessoais**
- **Ameaçam interromper informações críticas**

SPEAR PHISHING

- **Técnica simples que envia e-mail para pessoas específicas**
- **Informações importantes**

CIBERCRIMINOSOS

- **Roubam dados de cartão de crédito**
- **Ransomware**
- **A missão é espionar, extorquir e constranger**
- **Se infiltram em sistemas para roubar dados pessoais**
- **Ameaçam interromper informações críticas**

ATAQUE DE DIA ZERO

- **Utilizam qualquer método de exploração existente ou desenvolvem novos métodos por conta própria**
- **Descobrem novas vulnerabilidades não corrigidas em sistemas operacionais e/ou aplicações**


MAUS ATORES


hackone
NSE1: PERSPECTIVAS SOBRE A SEGURANÇA DE DADOS
NOME DO MENTOR: ALEXANDRE SABINO

SEGURANÇA DA INFORMAÇÃO

- **Acrônimo InfoSec**
- **Proteção de Dados: Segurança e Privacidade**
- **Privacidade está realcionada a políticas comerciais**
- **Segurança Cibernética protege redes, dispositivos e dados**

VULNERABILIDADES

- **Falhas no Software, Firmware ou Hardware**
- **Executam ações não autorizadas no sistema**
- **Aproveitam destes erros para infectar computadores com Malware**
- **Realizam outras atividades maliciosas**

INVASORES

- **Procuram explorar as vulnerabilidades**
- **Ações geralmente violam o uso pretendido do sistema**
- **As ameaças variam desde travessuras até roubo e alteração de informações**

SUPERFÍCIE DE ATAQUE

- **Local exposto em seu ambiente que um criminoso possa usar para entrar ou extrair algo valioso**
- **Depois de obter acesso, percorrem caminhos permitidos entre os dispositivos**
- **Profissionais de cibersegurança identificam as superficies para diminuir o risco de ataques**

MALWARE

- **Arquivo ou programa indesejado**
- **Vírus, Worm, botnet, cavalo de tróia, DDoS e ransomware**
- **Distribuição por e-mail, mídia social e sites comprometidos**

ENGENHARIA SOCIAL

- **Obter confiança e explorar o relacionamento**
- **Criminosos preferem o caminho com menor resistência**
- **Alavancam gatilhos emocionais como curiosidade, urgência e intimidação**

PROTEJA SEUS DADOS

- **Reconheça os riscos cibernéticos em potencial**
- **Informações confidenciais e altamente sensíveis precisam de proteção constante**
- **O crime cibernético é uma ameaça global e sem fronteiras**
- **Reguladores de Dados: GDPR e LGPD**
- **91% dos incidentes cibernéticos são causados por erro humano**


hackone
NSE1: PERSPECTIVAS DE SENHAS
NOME DO MENTOR: ALEXANDRE SABINO

SENHAS RUINS

123456789

!@#$%^&

QWERTY

666666

admin

12345

111111

Princess

abc123

123456

welcome

monkey

qwerty123

Password

PROTEJA SUAS SENHAS

- **Gerenciadores de Senhas**
- **Autenticação Multifatorial (MFA)**
- **Realizar backup constantemente**


hackone
NSE1: PERSPECTIVAS DE AMEAÇAS À INTERNET
NOME DO MENTOR: ALEXANDRE SABINO

AMEAÇAS À INTERNET

- As ameaças cibernéticas afetam sua experiência em:
  - Casa
  - Trabalho
  - Viagens
- A cada segundo 100 novos dispositivos IoT são conectados à Web
- Necessidade de conscientização de segurança

SEJA VIGILANTE

- Os criminosos confiam na Engenharia Social
- Engenheiro Social tem como objetivo obter sua confiaça
- Explorar o relacionamento para alcançar o objetivo

JUICE JACKING

- Estação de carregamento pública comprometida
- Aeroporto, estações de trem, arenas, áreas públicas
- Instalação de Malware

PHISHING

- E-mail armado que ser disfarça de reputação
- Atrai grupos-alvo a tomar decisão
- Exige que apenas uma vítima seja bem-sucedida

RANSOMWARE

- Malware que impede o acesso aos sistemas de computador
- E-mail é o vetor predominante de ataque
- Exige uma quantia em dinheiro

SPEARFISHING, WHALING, FRAUDE DE CEO e COMPROMETIMENTO DE E-MAIL COMERCIAL

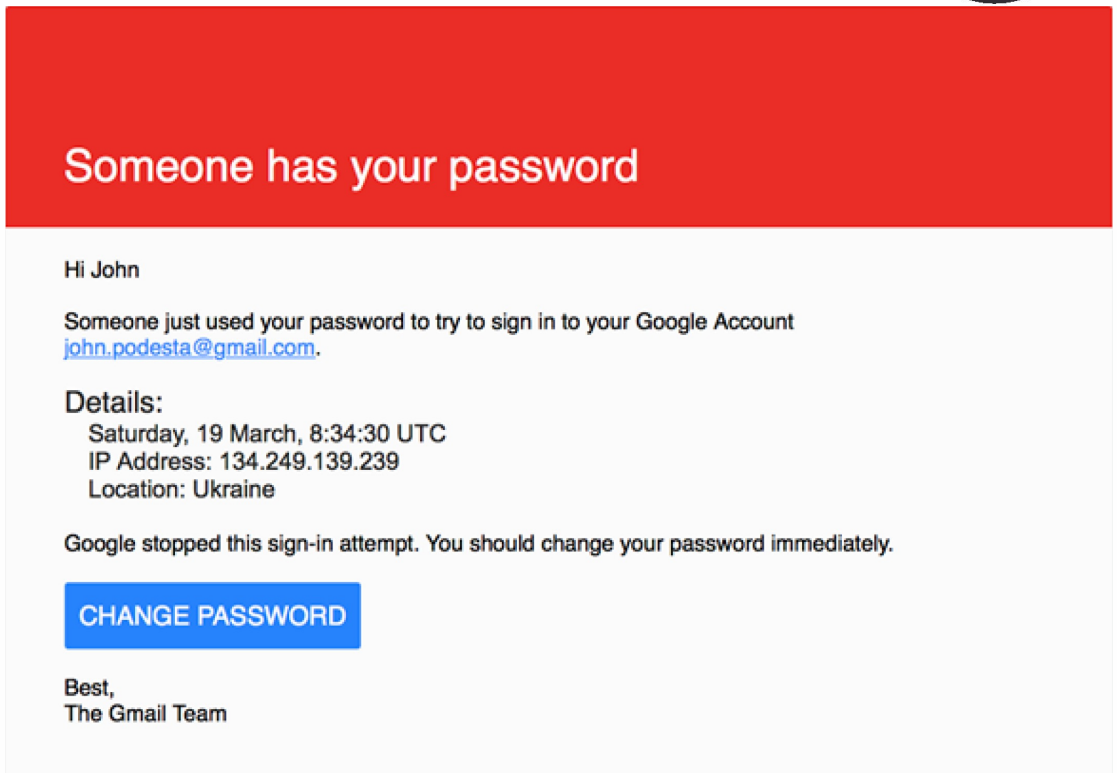
- **Mensagens Fraudulentas e armadas**
- **Visam uma função ou pessoa específica**
- **Geralmente são motivadas finaceiramente**

SEGURANÇA MÓVEL

- **Conduzem mais da metade do tráfego da Internet**
- **Alvos muito atraentes**
- **Existem uma infinidade de vulnarabilidades**
- **Wi-Fi é a principal ponto de entrada para os cibercriminosos entrarem**

ATENÇÃO

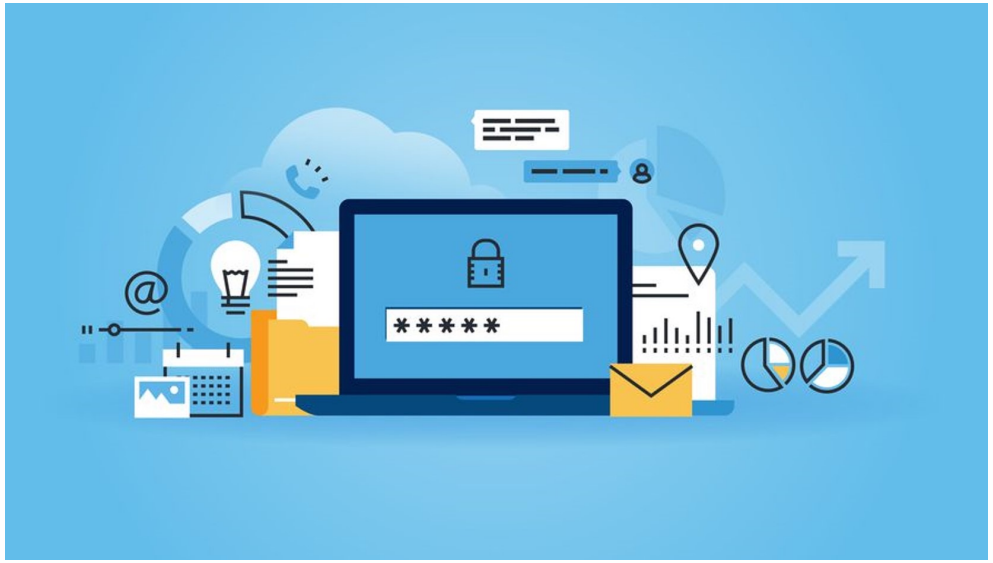
- **Antes de conectar a rede, confirme o nome da rede e os procedimentos de login**
- **Pontos de Acesso Público sempre são um risco de segurança**
- **E-mail é o vetor número 1 de infecção para todos os tipos de malware, inclusive o ransomware**
- **Ataques como Spearphishig, Whaling, Fraude de CEO são eficazes em 91% das vezes**




hackone
NSE1: PERSPECTIVAS DE AMEAÇAS INTERNAS
NOME DO MENTOR: ALEXANDRE SABINO

CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO

- Ameaças de segurança têm inúmeras origens
- Erro humano geralmente é a causa de todas as violações de segurança
- Sempre siga as políticas e diretrizes de manipulação dos dados
- Faça backup das informações sigilosas e essenciais em um dispositivo criptografado com senha forte
- Cuidado com bisbilhoteiros ou pessoas rodeando sua mesa com atitude suspeita



CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO

- **Não escreva ou deixe senhas em bilhetes colocados em sua mesa**
- **Não mantenha nenhuma informação confidencial e exclusive em sua mesa**
- **Bloqueie a tela do seu computador e do cellular sempre que se ausentar**
- **Comunique à equipe de segurança qualquer arrombamento de janela, portas ou outros itens trancados**
- **Denuncie atividades suspeitas na entrada e saída da empresa ou proximidades dela**

CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO

- **Denuncie entregas suspeitas e não abra e nem toque nas embalagens**
- **Rasgue e destrua todos os documentos que contenham informações sigilosas**
- **Use crachá para entrar no local de trabalho e nunca deixe alguém pegar “carona”**
- **Trate todos os dispositivos como sigilosos**

AMEAÇAS INTERNAS

- **Usuário interno: Tem acesso autorizado aos recursos da empresa**
- **Ameaça Interna: Risco de um usuário interno usar o acesso autorizado**
- **As ameaças internas são um dos vetores de ataque mais desafiadores de serem tratados**
- **Ameaça interna maiciosa sempre está ligada a empresa, e conscientemente faz dela um alvo para o ataque**
- **Toda a ameaça gira em torno de pessoas**


hackone