

**SEJA CIBERESPERTO**  
**#CyberMonth**



**MÊS DA CONSCIENTIZAÇÃO EM  
CIBERSEGURANÇA 2021**

# O que é o Mês da Conscientização em Cibersegurança?

O Mês da Conscientização em Cibersegurança aumenta a conscientização sobre a importância da cibersegurança em todo o país.





# Cibersegurança “E daí?”

## Você sabia?

Existem antivírus para dispositivos móveis, que são um alvo fácil e frequente para hackers e outros atores ruins.



## Cibersegurança e Bom senso

---

- Manter-se em segurança on-line não é muito diferente de manter-se em segurança no mundo físico!
- Mantenha a calma e confie nos seus instintos!



## Termos Comuns

---

- Ator ruim
- Hacker
- Ciberataque

# Faça sua parte. #BeCyberSmart

A cibersegurança  
começa com VOCÊ e  
é responsabilidade  
de todos.

No momento, estima-se haver  
**5,2 bilhões de usuários de internet, ou  
63% da população mundial.**



## Exemplos

- Roubo de identidade
- Materiais de abuso sexual de crianças
- Roubo financeiro
- Violações de propriedade intelectual
- Malware
- Engenharia social maliciosa

# CIBERCRIME



## O que é?

Cibercrime é qualquer crime cometido por meios eletrônicos.

Isso pode incluir...

- Roubo
- Fraude
- E até mesmo homicídio



## Por que se importar com isso?

- O crime é um perigo na internet e fora dela!
- Princípios básicos de autodefesa cibernética podem ajudar muito a manter você e seus dados fora das mãos de atores ruins.



# MALWARE

## Exemplos

- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Vírus
- Worms



## O que é?

Qualquer software feito para...

- Danificar
- Desabilitar
- Ou dar acesso não autorizado ao seu computador ou a outro dispositivo conectado à internet para alguém



## Por que se importar com isso?

- A maioria dos cibercrimes começa com algum tipo de malware. É quase certo que você, sua família e suas informações pessoais corram risco se um malware conseguir chegar ao seu computador ou aos seus dispositivos.



# RANSOMWARE



## O que é?

Malware feito para tornar os dados ou o hardware inacessíveis para a vítima até que ela pague um resgate.

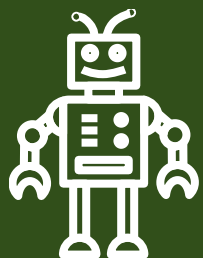
## Exemplos

- Cryptolocker
- Winlock
- Cryptowall
- Reveton
- Bad rabbit
- Crysis
- Wannacry



## Por que se importar com isso?

- Muitas vezes baixado na forma de links maliciosos de e-mail
- Danos à estabilidade financeira e à reputação
- Não há garantia de que você consiga recuperar os dados, mesmo pagando
- Muitas vezes usado como distração para outra atividade maliciosa



### Você sabia?

Nem todos os bots são ruins. Quando você usa um mecanismo de busca, os resultados são possíveis com a ajuda de bots que rastreiam a internet e fazem a indexação do conteúdo. Chatbots como Siri e Alexa são outro tipo comum de bot “bom”.

# BOTS



## O que é?

Os bots são um tipo de programa usado para tarefas automatizadas na internet.

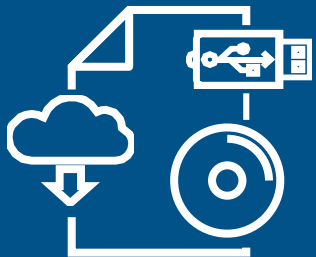


## Por que se importar com isso?

Os bots maliciosos podem:

- Recolher senhas
- Registrar pressionamentos de tecla
- Obter informações financeiras
- Apropriar-se de contas em redes sociais
- Usar o seu e-mail para enviar spam
- Abrir “portas dos fundos” no dispositivo infectado





### Você sabia?

Qualquer coisa conectada à internet é potencialmente vulnerável, desde patinetes elétricos até laptops e navios cargueiros.

# CIBERATAQUES FÍSICOS



## O que é?

Os ciberataques físicos usam hardware, dispositivos de armazenamento externo ou outros vetores de ataque físico para infectar, danificar ou comprometer sistemas digitais de alguma outra forma. Isso pode incluir...

- Dispositivos de armazenamento USB
- CD/DVD
- Internet das Coisas (IoT)



## Por que se importar com isso?

- Fácil de negligenciar
- Difícil de identificar e detectar
- Extremamente difícil de remover
- Pode fazer qualquer coisa, desde a instalação de ransomware e envio de cópias ou modificação de sistemas de informações até o desmantelamento de redes



# ENGENHARIA SOCIAL

## Exemplos

- Phishing
- Pretexting
- Baiting
- Quid pro quo
- Tailgating
- Trabalho interno
- Swatting



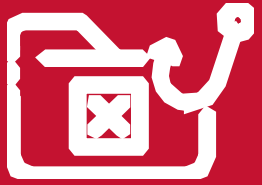
## O que é?

- Os cibercriminosos podem tirar vantagem de você, usando informações facilmente disponíveis por meio de...
- Plataformas de redes sociais
- Compartilhamento da localização
- Conversas em pessoa



## Por que se importar com isso?

- A sua privacidade não é só um luxo – é uma medida de segurança
- Os ataques podem ser bem-sucedidos com pouco ou nenhum conhecimento ou competência em programação
- As medidas tecnológicas de segurança só conseguem proteger você até certo ponto; você é a sua melhor defesa



# PHISHING



## O que é?

Mensagens falsas de uma fonte que parece confiável ou respeitável criadas para convencer você a...

- Revelar informações
- Dar uso não autorizado a um sistema
- Clicar em um link
- Se comprometer com uma transação financeira



## Por que se importar com isso?


- Extremamente comum
- Pode ter sérias consequências
- Preste atenção aos detalhes

## Exemplos

- E-mails
- Mensagens de texto
- Telefonemas
- Mensagens e postagens em redes sociais
- Hiperlinks suspeitos

# Este e-mail enganaria você?



 Nova mensagem — ↗ ✕


---

**De** Fonte-que-parece-legítima@quaseoseuemaildetrabalho.com

---

**Assunto** Atualização urgente de TI: vulnerabilidade de software


---

 Atualização de software







Boa tarde, Tom,

Identificamos uma vulnerabilidade em “Software Famoso” que permite que um invasor registre chamadas e vídeos do seu computador sem o seu conhecimento. Instale a atualização de ataque até o fim do dia ou sua estação de trabalho será bloqueada.

Também criamos um aplicativo para que todos os funcionários determinem se foram afetados por essa vulnerabilidade. Clique [aqui](#) para rodar o aplicativo.

Sinceramente,  [www.fakewebsite.com/gotcha.exe](http://www.fakewebsite.com/gotcha.exe)  
Chefe Clique ou toque para seguir o link.  
Departamento de TI da sua Empresa

---

**RESPONDER**      



## Exemplos

Sua localização está embebida na forma de metadados em toda foto que você tira com o telefone. Desligue os serviços de localização quando não estiver usando esses serviços para dificultar a visualização dessas informações por atores ruins.

# SWATTING



## O que é?

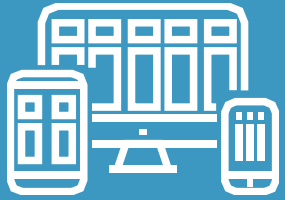
Um ataque centrado no compartilhamento da localização no qual atores ruins ligam para a polícia e alegam que a vítima cometeu um crime...

- Ameaça de bomba
- Invasor armado
- Incidente violento



## Por que se importar com isso?

- Consequências físicas e imediatas
- Às vezes a intenção é apenas fazer uma pegadinha
- O resultado pode ser prisão e lesões graves
- Para reduzir o risco, compartilhe sua localização somente com indivíduos confiáveis, e só compartilhe as fotos das férias após ter voltado para casa com segurança



# OUTRAS ROTAS DE ATAQUE

## Exemplos

- Dispositivos inteligentes
- Telefone celular
- Termostato
- Veículos
- Consoles de jogo
- Impressoras
- Equipamento médico
- Sistemas industriais



## O que é?

- Internet de todas as coisas
- Qualquer dispositivo conectado à sua rede
- Coleta de informações
- Acesso remoto
- Bluetooth
- Portas abertas



## Por que se importar com isso?

- Sua rede pode ser usada para atacar outra pessoa
- Qualquer dispositivo que armazene informações ou esteja conectado à internet pode ser uma vulnerabilidade
- Assuma que você está vulnerável, e tome medidas para entender e reduzir o risco
- Não seja um alvo fácil

# Como você pode se proteger melhor on-line?



## Proteja suas redes.

Roteadores sem fio são uma forma de acesso aos dispositivos on-line por cibercriminosos.



## Mantenha tudo atualizado.

Mantenha o software atualizado na última versão e configure o software de segurança para fazer varreduras regulares.



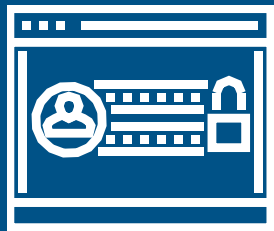
## Tudo que você conecta deve ser protegido.

Uma defesa comprovada contra a invasão é atualizar para o software de proteção contra vírus mais recente.



## Dobre sua proteção de login.

Habilite a autenticação multifator (MFA) para garantir que a única pessoa com acesso à sua conta seja você.



# Dicas de senha

## Você sabia?

Preenchimento (stuffing) de credenciais ou senhas é um ciberataque que usa nomes de usuário e senhas comprometidas de um site para preencher outro, na esperança de que o usuário utilize as mesmas informações de login em várias plataformas.

\*\*\*\*\*

**Use senhas diferentes em sistemas e contas diferentes**

\*\*\*\*\*

**Use a senha mais longa possível**

\*\*\*\*\*

**Use uma mistura de maiúsculas e minúsculas, números e símbolos**

\*\*\*\*\*

**Redefina a senha a cada dois ou três meses**

\*\*\*\*\*

**Use um gerenciador de senha**



# Tema do Mês da Conscientização em Cibersegurança

Tema:

- Faça sua parte.  
#BeCyberSmart.



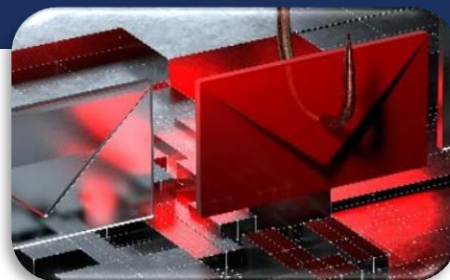
# Cronograma do Mês da Conscientização em Cibersegurança 2021



**1º de outubro:**  
Lançamento  
oficial



**SEMANA 1:**  
**Semana de 4  
de outubro**  
Seja ciberesperto.



**SEMANA 2:**  
**Semana de 11  
de outubro**  
Lute contra o phishing!



**SEMANA 3:**  
**Semana de 18  
de outubro**  
Explore. Experimente.  
Compartilhe. (Semana  
de Conscientização  
sobre Carreiras em  
Cibersegurança)



**SEMANA 4:**  
**Semana de 25  
de outubro**  
Cibersegurança em  
primeiro lugar

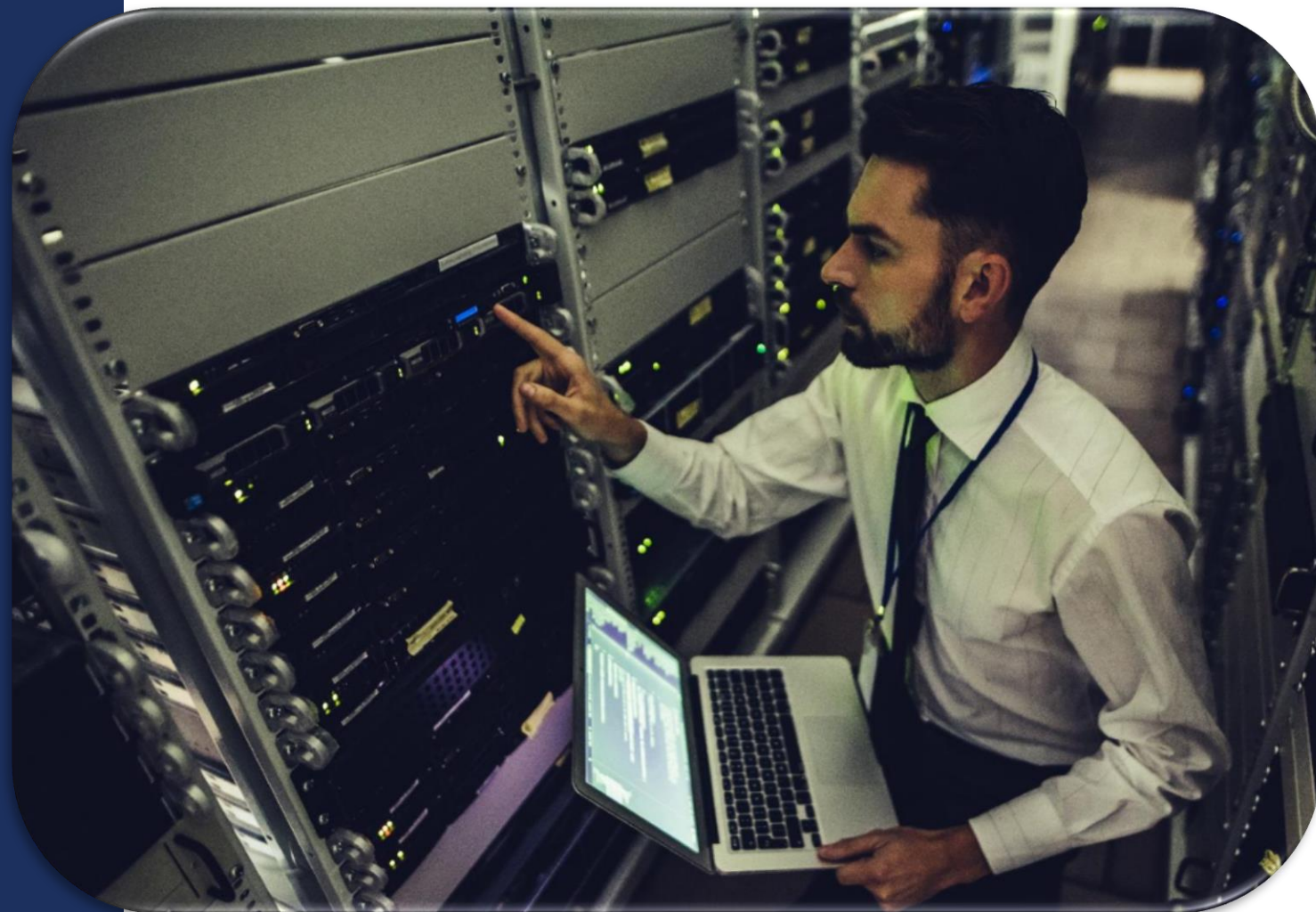
# Semana 1: Seja ciberesperto.



**Semana 2:**  
**Lute contra**  
**o phishing!**



**Semana 3:**  
**Explore.**  
**Experimente.**  
**Compartilhe.**  
**Semana de**  
**Conscientização**  
**sobre Carreiras em**  
**Cibersegurança**



**Semana 4:**  
**Cibersegurança**  
**em primeiro lugar.**





## **Estimule a conscientização e envolva-se**

- **Promova o Mês da Cibersegurança**
- **Promova o Mês da Conscientização em Cibersegurança nas redes sociais; use a hashtag [#BeCyberSmart](#)**
- **Voluntarie-se para palestrar em eventos do Mês da Conscientização em Cibersegurança**
- **Passe as dicas de cibersegurança para amigos, familiares e colegas**

**Para mais informações, entre em contato  
com [CyberAwareness@cisa.dhs.gov](mailto:CyberAwareness@cisa.dhs.gov)**

Acesse [cisa.gov/cybersecurity-awareness-month](https://cisa.gov/cybersecurity-awareness-month) ou  
[staysafeonline.org/cybersecurity-awareness-month/](https://staysafeonline.org/cybersecurity-awareness-month/)  
para encontrar mais recursos.