



Grupo de Resposta a Incidentes de Segurança

Segurança em Códigos QR

GRIS



Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

Quem somos?



Quem somos?

- **CSIRT acadêmico** criado em 2003
 - .Não era nada em 2003 para UFRJ
 - .Atualmente, referência em SI na universidade



GRIS

Quem somos?

- Formado **por alunos** da UFRJ
 - . Inicialmente, formado por alunos da graduação de Ciência da Computação
 - . Atualmente, qualquer aluno da universidade que passe na prova do Processo Seletivo

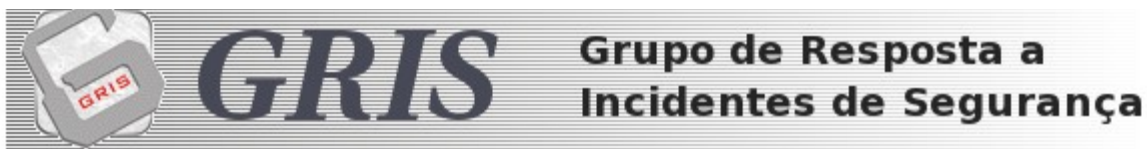
Quem somos?

- Resultados

- . Artigos**
- . Tutoriais**
- . Dicas**
- . Palestras**
- . Mini-cursos**
- . Membros e ex-membros em grandes empresas**
- . Empresas criadas**

Quem somos?

gris.dcc.ufrj.br



Buscar no Site
☐ apenas nesta seção



Você está aqui: [Página Inicial](#)

Sobre o GRIS

O GRIS - Grupo de Resposta a Incidentes de Segurança - atua no [Departamento de Ciência da Computação](#) da [Universidade Federal do Rio de Janeiro](#) e em outras unidades solicitantes da Universidade. Tem como objetivo a detecção, resolução e prevenção de incidentes de segurança, além de oferecer suporte acadêmico aos estudantes da UFRJ que possuam interesse particular na área de segurança da informação.

Dentre as principais atividades do GRIS estão:

- Aplicar atualizações de segurança

Redes Sociais



Dia Internacional de Segurança da Informação



Segurança em Códigos QR - Agenda

1 – Códigos QR?

- 1.1 – O que são?
- 1.2 – Códigos QR x Códigos de Barra
- 1.3 – Aplicações no dia a dia

2 – É seguro escanear Códigos QR?

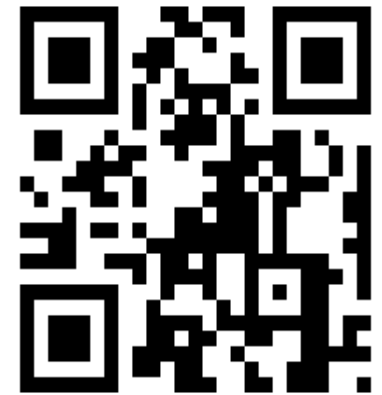
- 2.1 – Por que me atacariam?
- 2.2 – Nossa maior falha
- 2.3 – Exemplos de possíveis ataques
- 2.4 – Casos famosos
- 2.5 – SQRC

3 – Estudo de Caso: exemplo de ataque

4 – Boas práticas

- 4.1 – Para quem escaneia
- 5.2 – Para quem quer criar Códigos QR

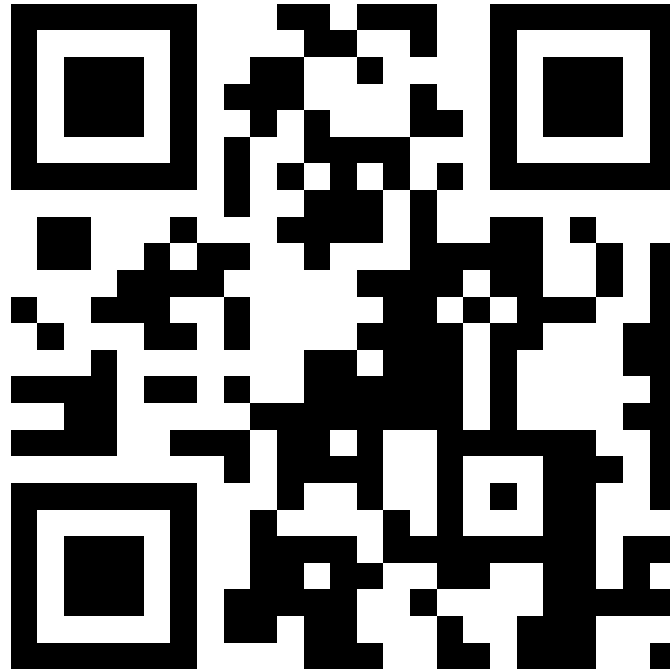
5 – Projetos futuros





Códigos QR?

O que são Códigos QR?



Desenvolvido no Japão em 1994 pela DENSO CORPORATION, os códigos QR(Quick Response) são utilizados para transmitir qualquer tipo de dado através de uma simples captura de imagens em 2D.

Atualmente, os códigos QR estão ganhando uma popularidade muito grande pela sua praticidade e devido ao mercado de dispositivos móveis, aparelhos capazes de lerem os códigos, estar crescendo muito!

Códigos? Eu já conheço um...





V
S



Códigos QR x Códigos de Barra

Qual a diferença de um Código QR para um Código de Barra?

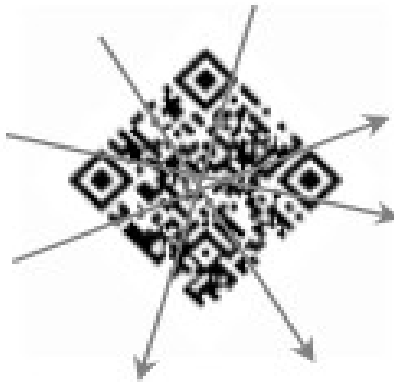
1) Posição onde são armazenados os dados



Códigos QR x Códigos de Barra

2) Leitura em alta velocidade e em 360°

Código QR



Leitura em 360°

Código de Barras



Leitura horizontal



Códigos QR x Códigos de Barra

3) Durabilidade contra manchas e danos

Código QR



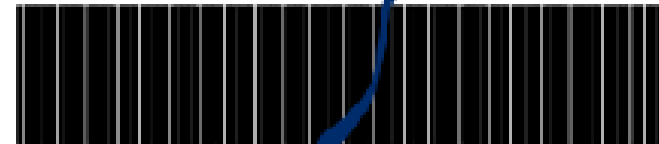
Manchado



Danificado

Leitura é possível

Código de Barras



Manchado

Leitura não é possível



Códigos QR x Códigos de Barra

4) Representação Kanji

Código QR

財団法人
流通システム
開発センター



Caracteres japoneses

Código de Barras



Apenas alfanuméricos





Códigos QR no dia a dia

Aplicações no dia a dia

Cada vez mais nos deparamos com Códigos QR por aí!
Vejam alguns exemplos:

1) Publicidade



Aplicações no dia a dia

2) Hospitais



Aplicações no dia a dia

3) Mercados

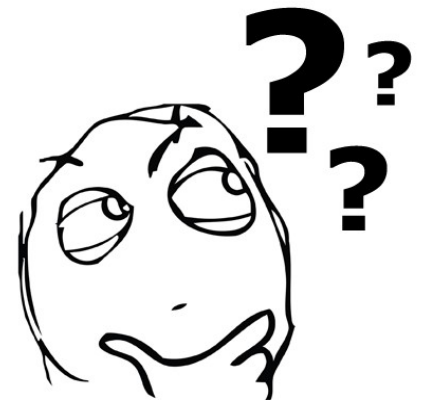


Aplicações no dia a dia

4) Pagando contas



É seguro escanear Códigos QR?



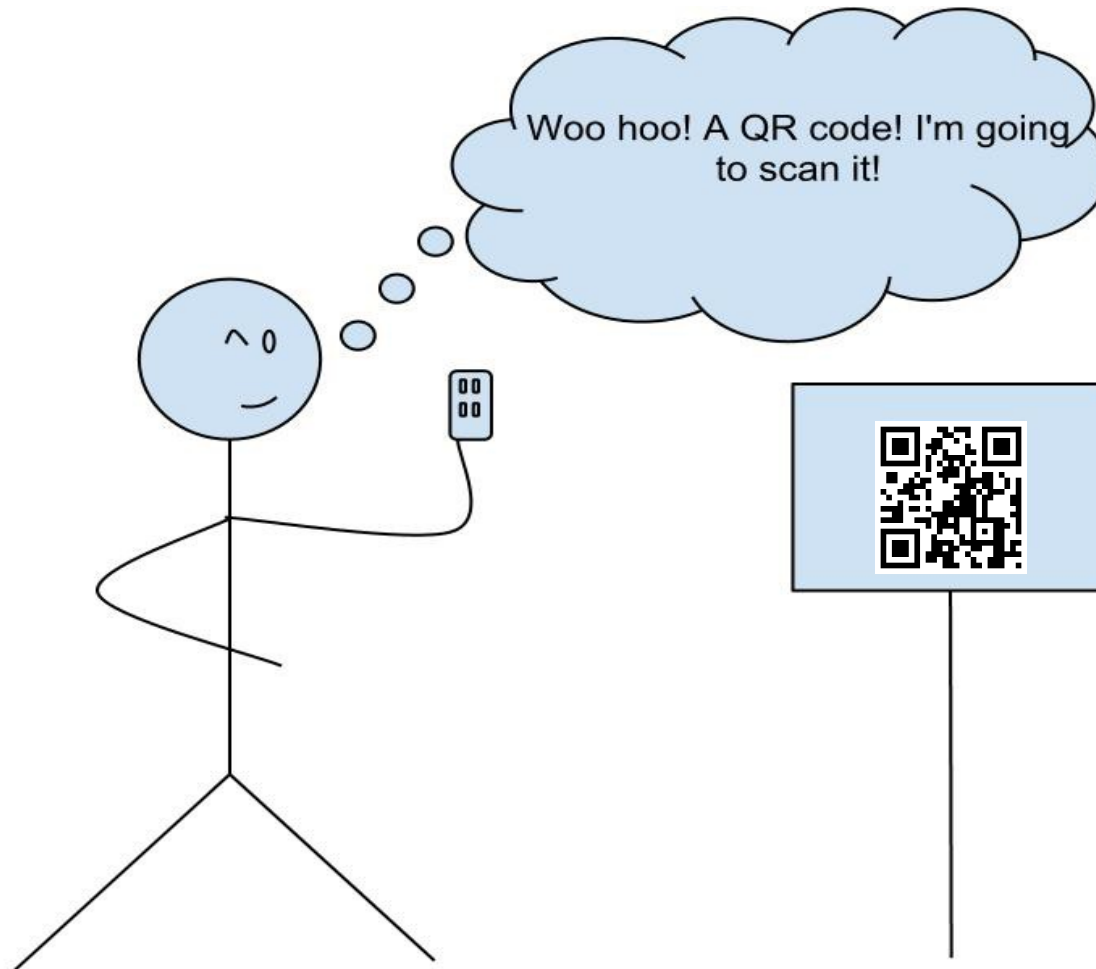
Por que me atacariam?



**Dispositivos móveis são uma
mina de ouro!**



Nossa grande falha



Curiosidade!





Possíveis ataques

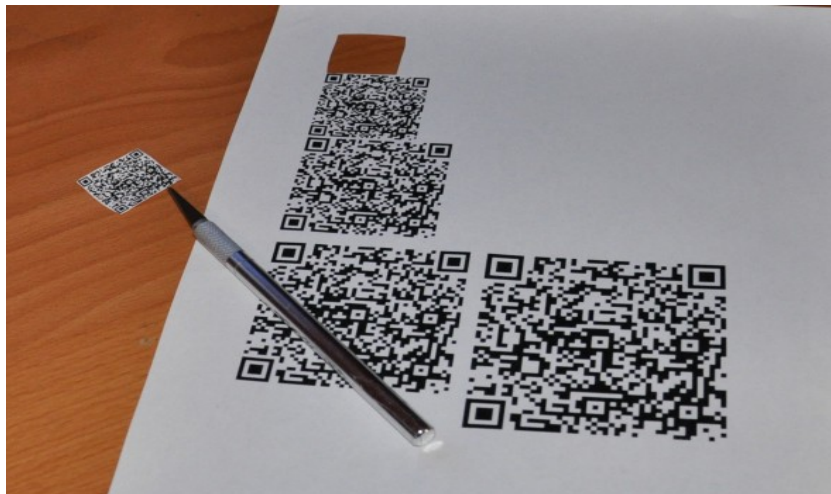
Exemplos de possíveis ataques

1) QRJacking



Exemplos de possíveis ataques

<http://notdanwilkerson.wordpress.com/2011/05/03/qr-jacking/>



Exemplo de ataques

2) ScanJacking



Boo!



Boa Tarde!



Exemplo de ataques

2) ScanJacking

		password
Syndication feed reader	feed:<url>	N/A
Apple FaceTime	facetime:<number>	N/A
Skype client	skype:<username number>?	add
	query	call

URL	skype:echo123?call
To	http://tinyurl.com/echo123skype



Exemplo de ataques

3) Phishing e Spear Phishing



Componente de segurança

Componente adicional de segurança

Prezado Cliente, **Pessoa Física e Jurídica:**

Foi lançada uma nova ferramenta para proteger ainda mais seu acesso online; Esta atualizará os módulos de proteção já existentes no seu computador, para um acesso seguro à sua conta pelo **portal** <http://www.bb.com.br> e pelo **Gerenciador Financeiro**.

A instalação é simples, rápida e segura. Basta clicar no link abaixo, e em seguida no botão Executar na janela que se abrirá e seguir as instruções no programa de instalação.

[> Clique aqui para instalação do Componente](#)

Atenção: Todos os usuários devem instalar o **Componente Adicional de Segurança**. Caso contrário seu computador será bloqueado para acesso online e o desbloqueio poderá ser realizado somente nas agências bancárias.


Em caso de dúvidas, ligue para Central de Atendimento BB,
Capitais e Regiões Metropolitanas: 4004 0001
Demais localidades: 0800 729 0001

» Banco do Brasil



Exemplo de ataques

4) Fraude de SMS



Save this code to add it to your blog or your documents.

You can also use the code's [permalink](#), or copy-paste the following HTML code:

```

```

QR-CODE GENERATOR

Content type:

☐ URL ☐ Text ☐ Phone Number ☒ SMS

Content:





Nr: +55999999999

Message: 154 characters left
GANHEI

Size: L ▼

Generate!

[Donate](#)



Exemplo de ataques

5) Conectando-se em rede inseguras

Conecte-se à
Internet sem fio
de graça:



Exemplo de ataques

6) ?? 7) ?? 8) ??
9) ??



Casos de ataques famosos



Casos conhecidos

1) th3j35t3r



boondock saint

@th3j35t3r

Hactivist for good. Obstructing lines of communication for terrorists, sympathizers, fixers, facilitators. No botnets here. I'll do my own dirty.

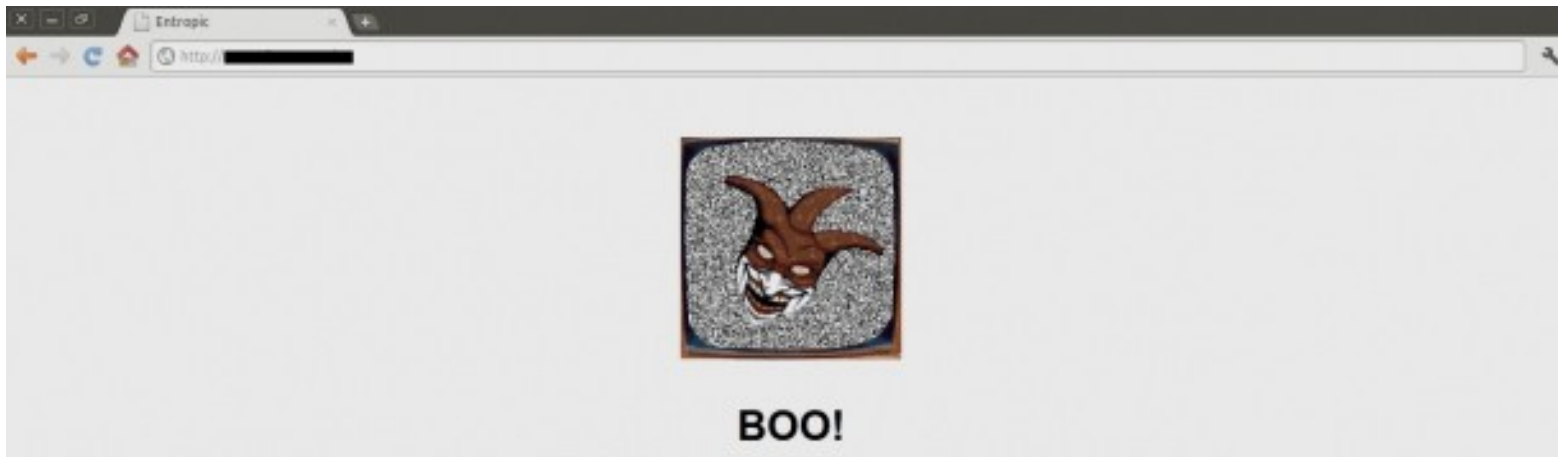
Behind you. <http://tinyurl.com/jesterblog>

Edit your profile

1,139 TWEETS

435 FOLLOWING

29,707 FOLLOWERS



Casos conhecidos

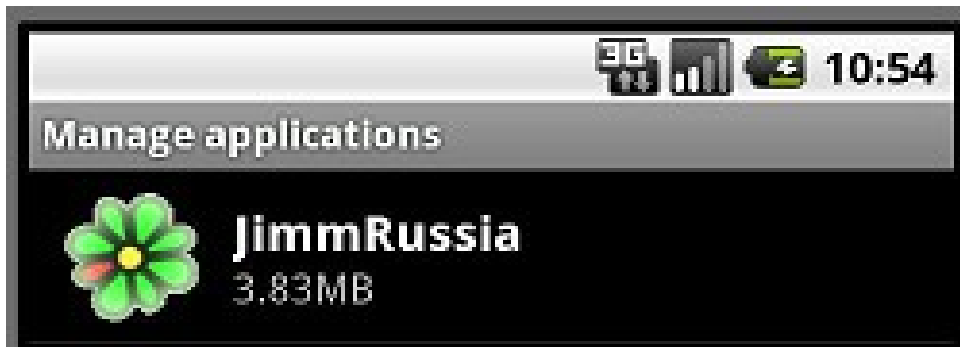
Alguns dados sobre o ataque:

- Mais de 1200 pessoas escanearam o código malicioso;
- Desses, 500 conseguiram ser de fato atacados;
- E desses 500, um número significativo estava na “shit-list”;
- Um arquivo .txt com 146 MB foi divulgado com todas as informações das vítimas do ataque.



Casos conhecidos

2) JimmRUssia



- O nome do pacote do malware: “appinventor.ai_russ_support.JimmRussia”

```
package="appinventor.ai_russ_support.JimmRussia"
```

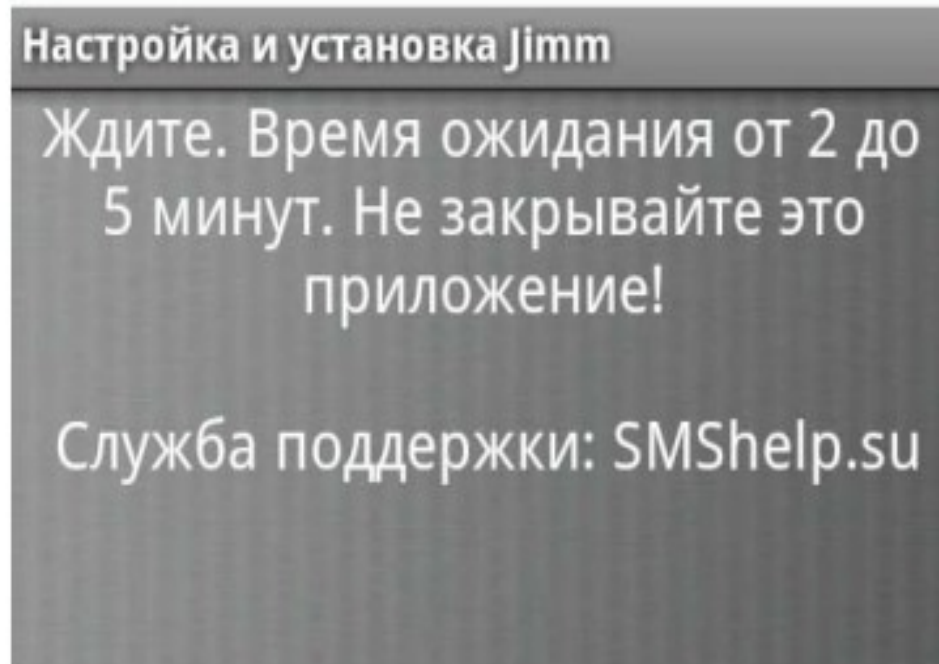
- Permissões requeridas pelo malware:

```
<uses-permission android:name="android.permission.SEND_SMS" />  
<uses-permission android:name="android.permission.INTERNET" />  
<uses-permission android:name="android.permission.RECEIVE_SMS" />
```



Casos conhecidos

- Depois de abrir o malware:



- Envio de SMS para “premium numbers”
- Redirecionamento para uma URL para um download de um arquivo malicioso





SQRC

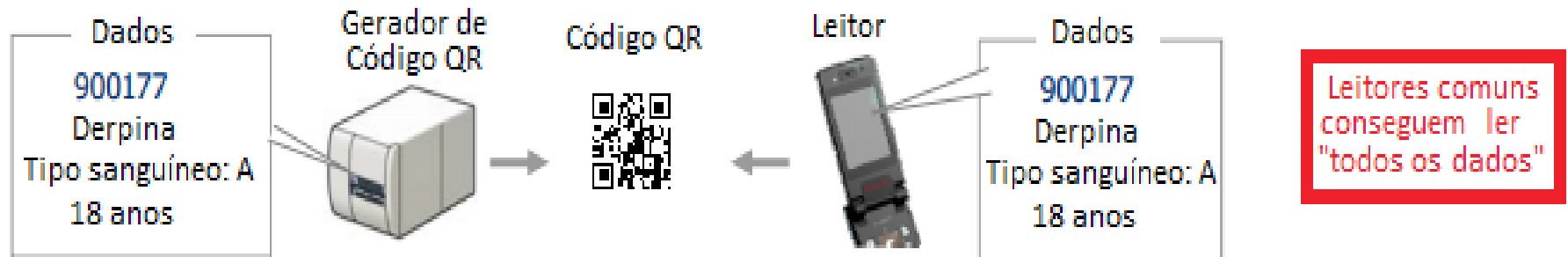
GRIS

Security Quick Response Code

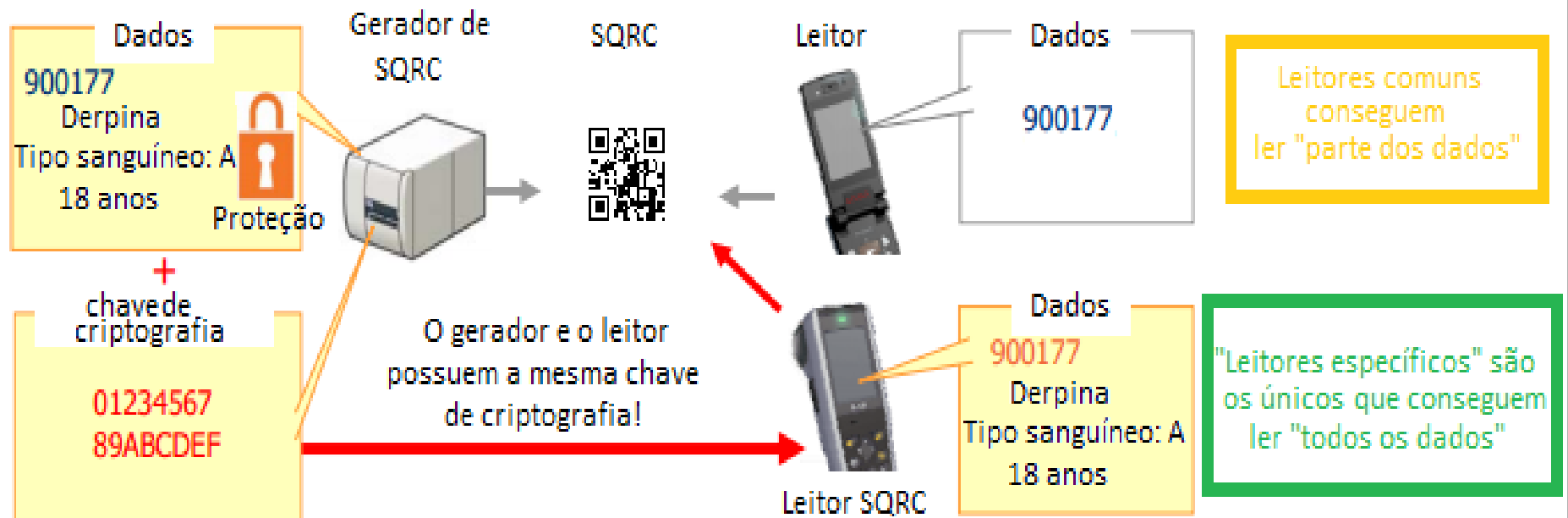


Security Quick Response Code

Código QR comum



SQRC



Security Quick Response Code



Estudo de Caso: exemplo de ataque



Estudo de caso: exemplo de ataque



A seguir será mostrado apenas uma **SIMULAÇÃO** de ataque utilizando QR Codes!



Estudo de caso: exemplo de ataque



Estudo de caso: exemplo de ataque

Planejando o ataque:

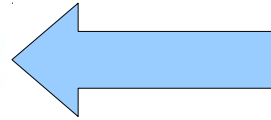
- 1) Escolher uma vítima;**
- 2) Colher informações da vítima;**
- 3) Engenharia Social através da coleta;**
- 4) Coleta de informações pessoais.**



Estudo de caso: exemplo de ataque

1) Escolher uma vítima

Subject : QRCode formulario - Novo
Formwidget-2 : Fulano
Formwidget-3 : fulano@email.com
Formwidget-6 : Iphone 5



[Generate Report here](#)
[Unsubscribe](#) from receiving this email

you'd like to unsubscribe and stop receiving these emails [click here](#).



Estudo de caso: exemplo de ataque

1) Escolher uma vítima

```
AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30  
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like  
Gecko) Version/6.0 Mobile/10A403 Safari/8536.25
```

```
Mozilla/5.0 (Linux; U; Android 2.3.6; pt-br; MB860 Build/4.5.2A-51_OLL-48)  
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1  
Mozilla/5.0 (Linux; U; Android 2.3.6; pt-br; MB860 Build/4.5.2A-51_OLL-48)  
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1  
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like  
Gecko) Version/6.0 Mobile/10A403 Safari/8536.25  
unknown AppEngine-Google; (+http://code.google.com/appengine; appid: qmksync)  
unknown AppEngine-Google; (+http://code.google.com/appengine; appid: qmksync)  
unknown AppEngine-Google; (+http://code.google.com/appengine; appid: qmksync)
```

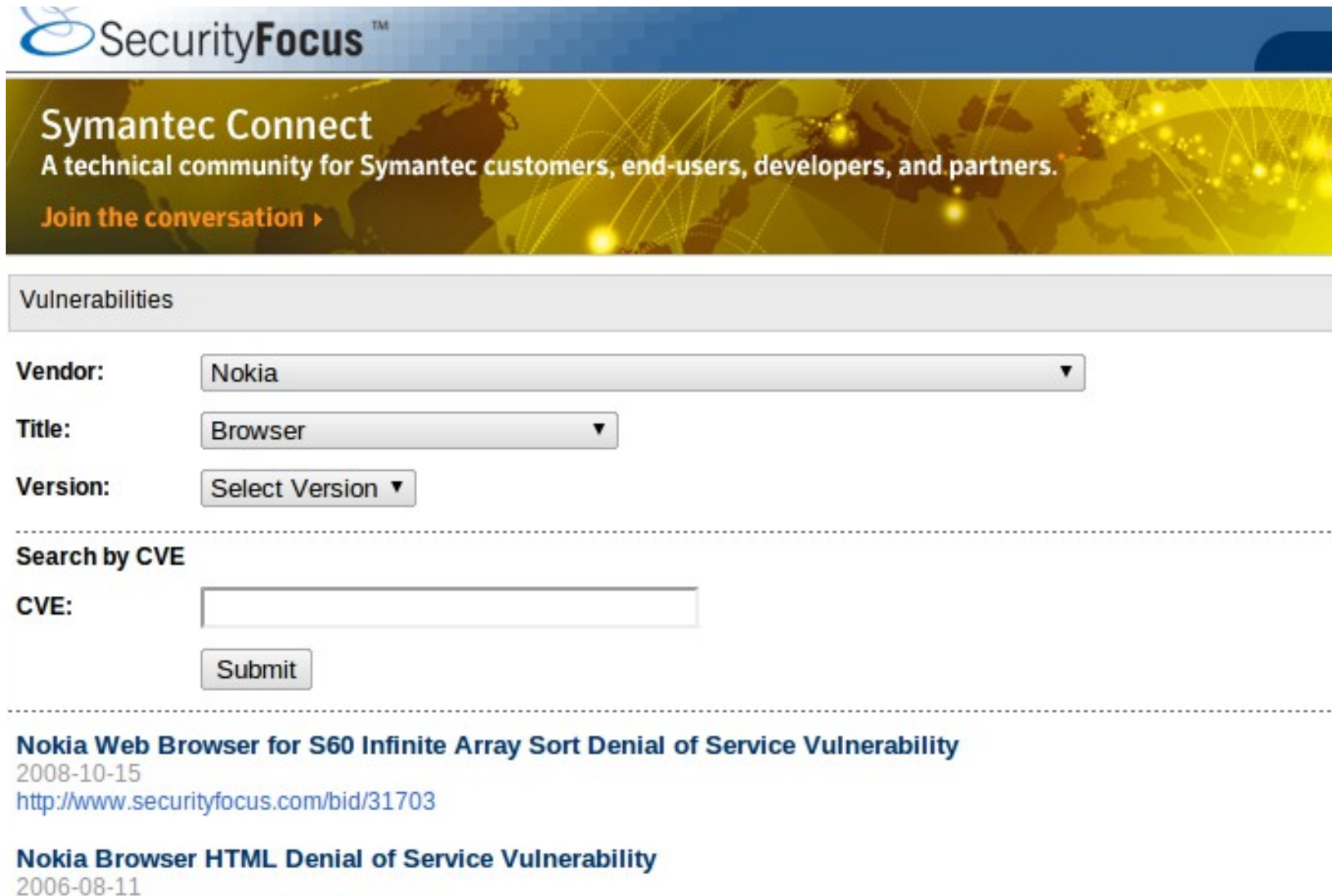
ZXing (Android)

```
Mozilla/5.0 (SymbianOS/9.4; Series60/5.0 Nokia5230-1d/50.4.001; Profile/MIDP-2.1  
Configuration/CLDC-1.1 ) AppleWebKit/533.4 (KHTML, like Gecko) NokiaBrowser/7.3.1.25  
Mobile Safari/533.4 3gpp-gba
```



Estudo de caso: exemplo de ataque

1) Escolher uma vítima



SecurityFocus™

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
[Join the conversation >](#)

Vulnerabilities

Vendor:

Title:

Version:

Search by CVE

CVE:

Nokia Web Browser for S60 Infinite Array Sort Denial of Service Vulnerability
2008-10-15
<http://www.securityfocus.com/bid/31703>

Nokia Browser HTML Denial of Service Vulnerability
2006-08-11



Estudo de caso: exemplo de ataque

2) Colher informações da vítima

Fulaninho da Silva Adicionar instituição de ensino Registro de atividades

trabalha na empresa **Empresa Super Importante**
lora em **São Paulo**
Adicione sua instituição de ensino
Adicione sua cidade natal

Amigos Fotos Mapa 1 Opções "Curtir" 1

Atividades Recente


Fulaninho adicionou **Clube de Regatas do Flamengo** aos times favoritos dela.

Fulaninho adicionou um emprego em **Empresa**



Estudo de caso: exemplo de ataque

3) Engenharia Social através da coleta

Notícias do Mengão no seu celular!  1

Ocultar detalhe

DE:

PARA:

Quinta-feira, 18 de Outubro de 2012 20

Quer receber notícias do Mengão no seu celular??

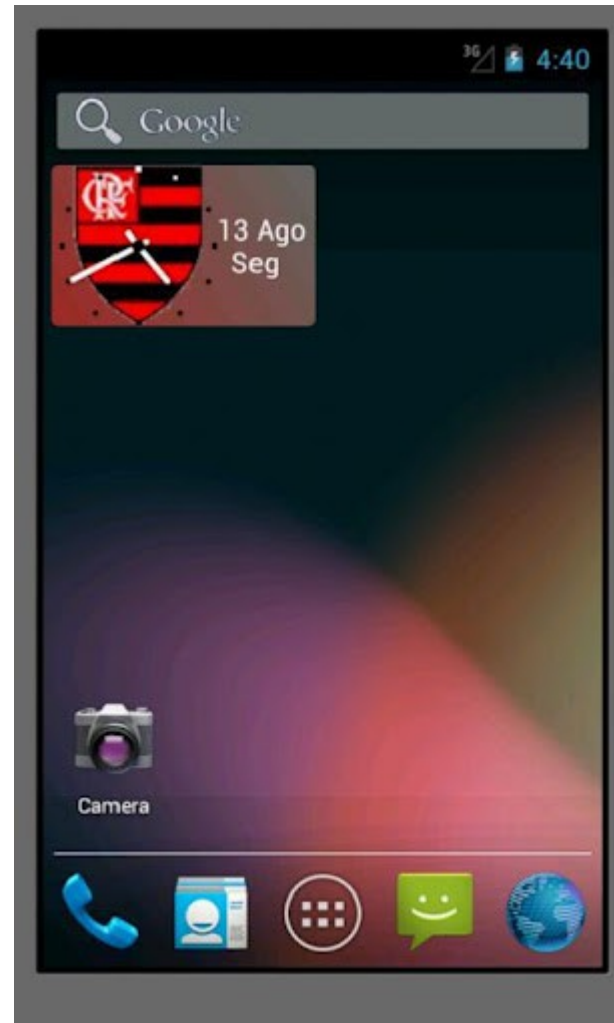
Instale agora o aplicativo Mengão Hexa em seu celular e receba diariamente notícias do Mais Querido do Brasil!

Basta escanear o QR Code abaixo:



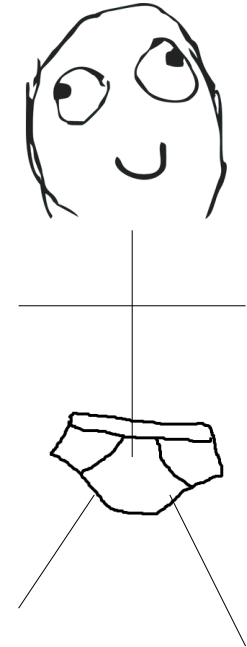
Estudo de caso: exemplo de ataque

3) Engenharia Social através da coleta



Estudo de caso: exemplo de ataque

4) Coleta de informações pessoais



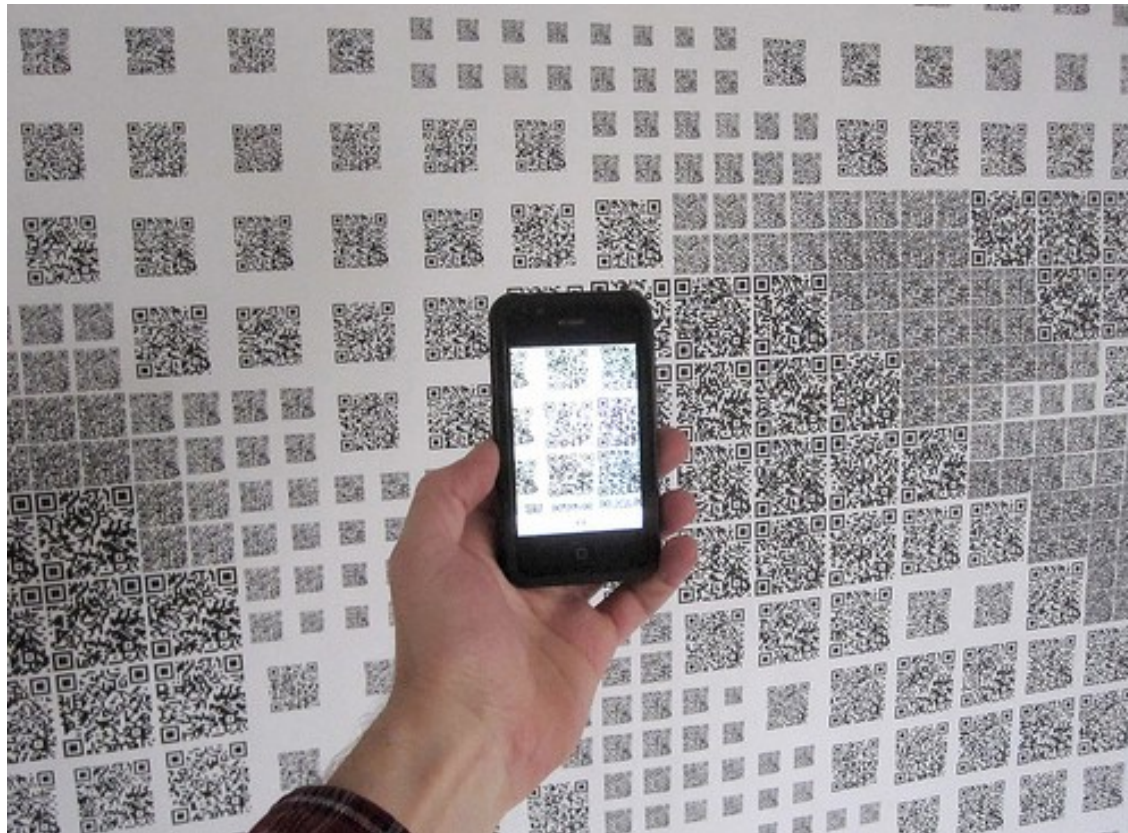


Boas Práticas

GRIS

Boas Práticas

Para quem escaneia



Boas Práticas

1) Utilize um bom leitor



You can share data by displaying a barcode on your screen and scanning it with another phone.



Application

Bookmark

Contact

Clipboard

Or type some text and press Enter



Boas Práticas

2) Não deixe um código QR agir sozinho!



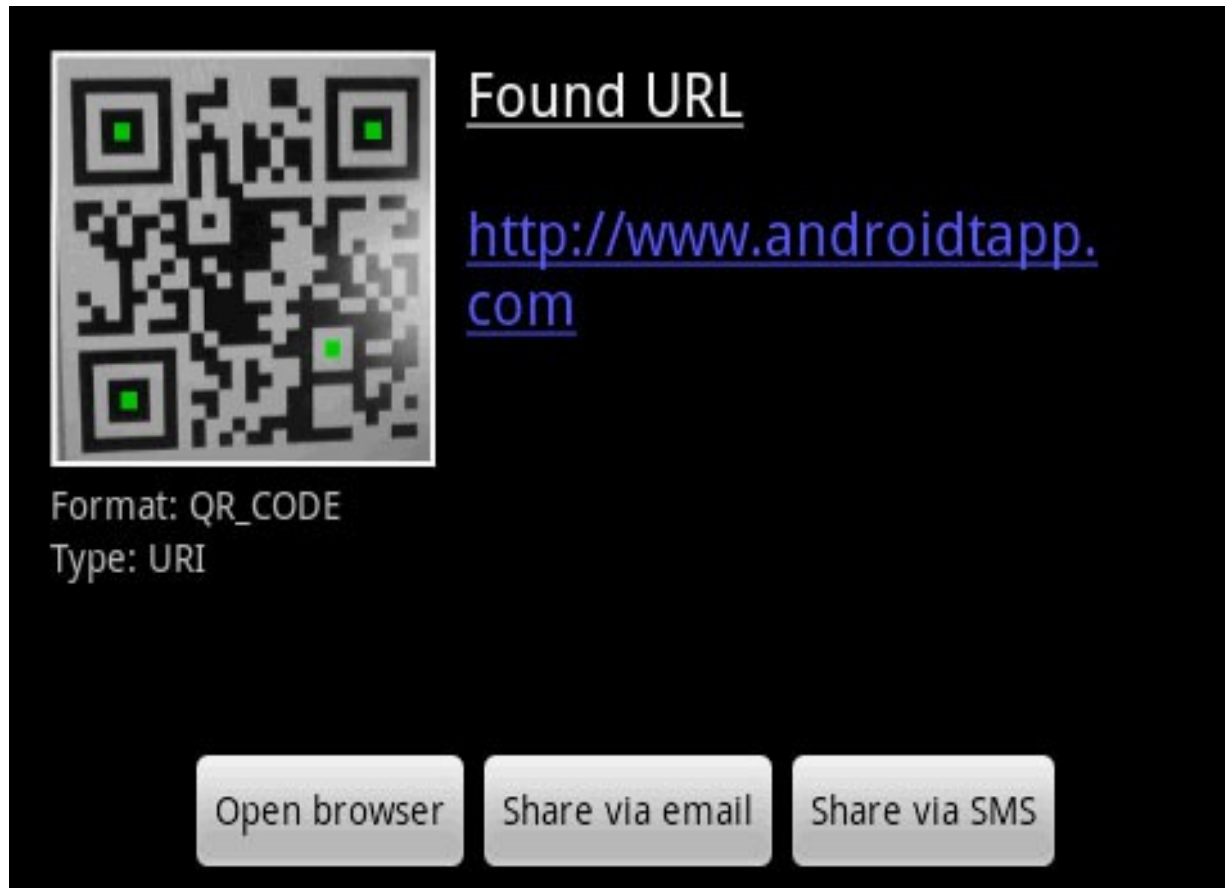
Boas Práticas

3) Não forneça informações desnecessárias



Boas Práticas

4) Sempre verifique a URL!



Boas Práticas

5) Verifique a integridade física do Código



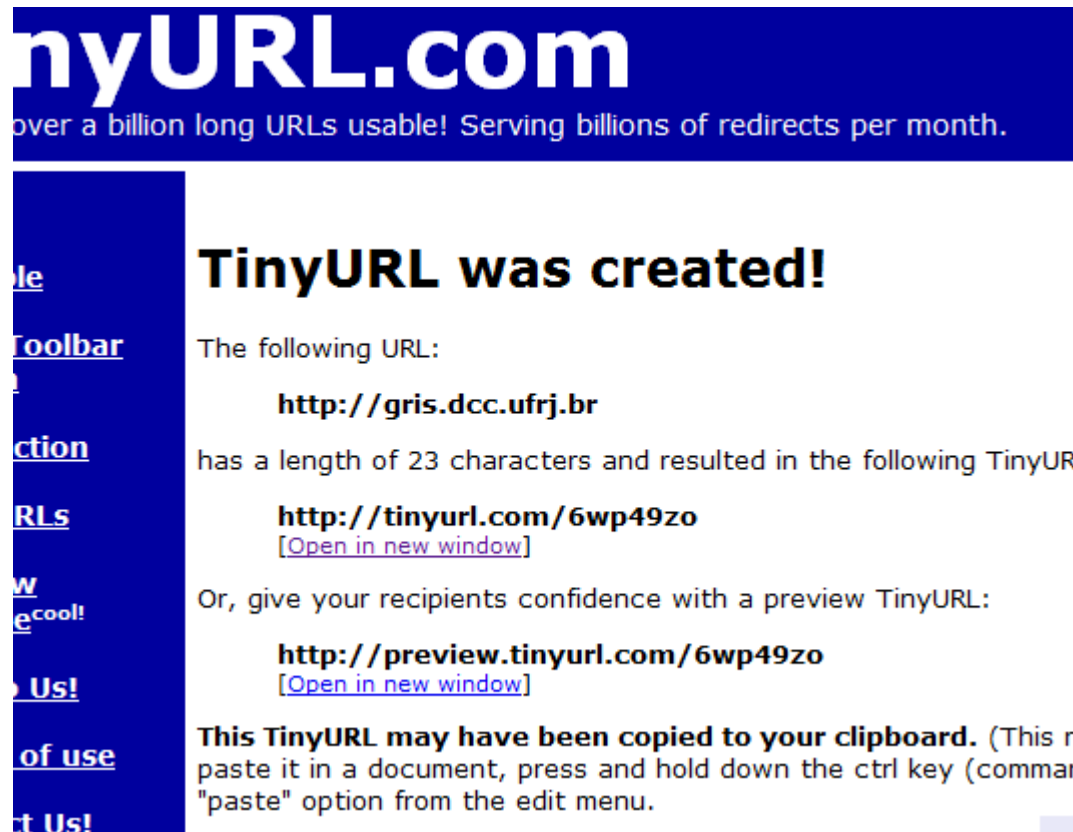
Boas Práticas

Para quem quer criar Códigos QR



Boas Práticas

1) Evite serviços de encurtamento de link!



nyURL.com
over a billion long URLs usable! Serving billions of redirects per month.

TinyURL was created!

The following URL:

<http://gris.dcc.ufrj.br>

has a length of 23 characters and resulted in the following TinyUR

<http://tinyurl.com/6wp49zo>
[\[Open in new window\]](#)

Or, give your recipients confidence with a preview TinyURL:

<http://preview.tinyurl.com/6wp49zo>
[\[Open in new window\]](#)

This TinyURL may have been copied to your clipboard. (This r
paste it in a document, press and hold down the ctrl key (commar
"paste" option from the edit menu.



Boas Práticas

2) Sempre mostre o endereço que seu Código redireciona e diga o que ele faz

Escaneie para entrar no site do GRIS e conhecer nossos projetos:



gris.dcc.ufrj.br



Boas Práticas

3) Não utilize Códigos QR para informações sensíveis



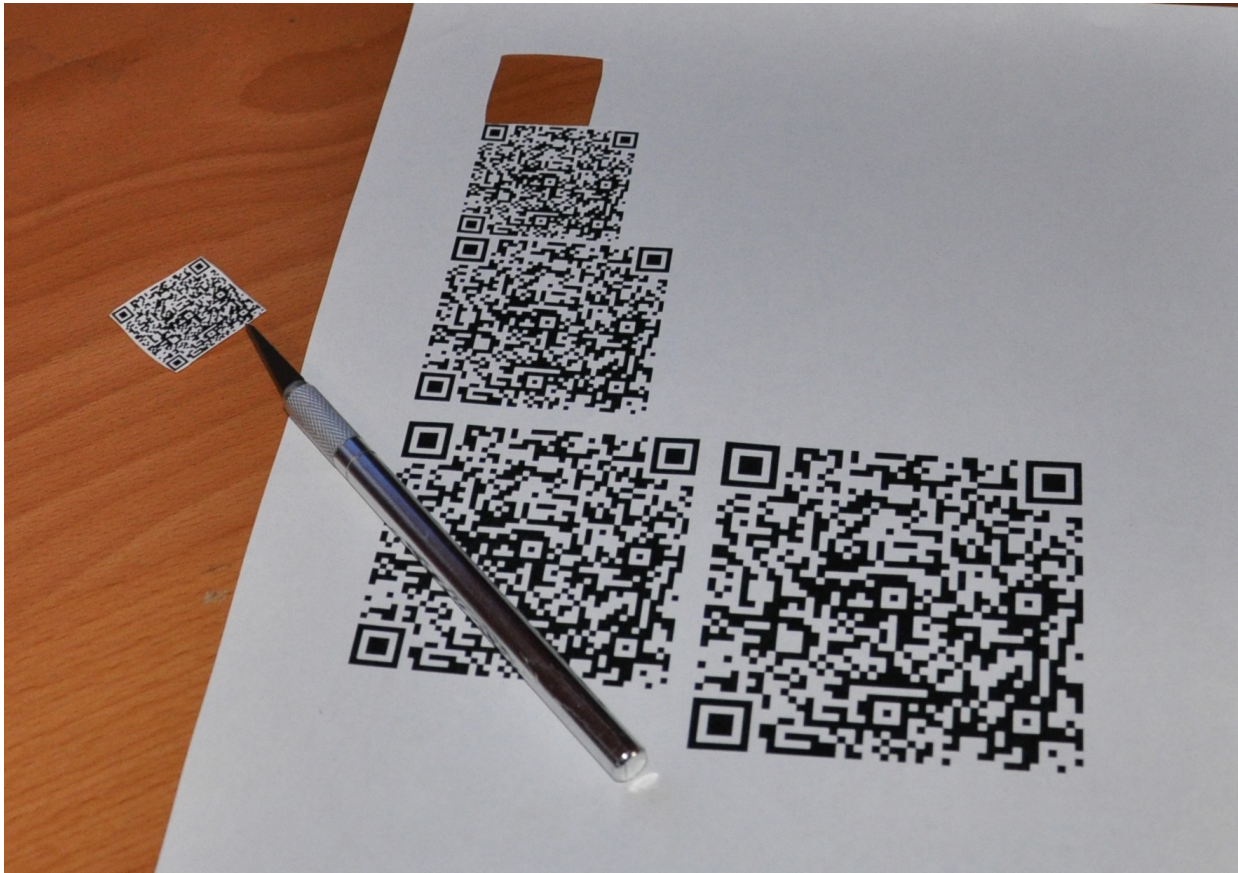
Boas Práticas

4) Procure zelar pela integridade física de seu Código QR



Boas Práticas

5) Tenha consciência de que pessoas podem fazer ataques!





Projetos Futuros

Projetos Futuros



- 1) Listar todas as vulnerabilidades recentes dos leitores de Códigos QR;
- 2) Pesquisar mais sobre a utilização do SQRC;
- 3) Conscientização intensa sobre a utilização dos Códigos QR;
- 4) Pesquisar sobre ataques recentes utilizando os Códigos QR;
- 5) Hacktivismo + Código QR ?? ;
- 6) Novas versões de Códigos QR e novos códigos.



Segurança em Códigos QR



Dúvidas?



Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

Segurança em Códigos QR



Obrigado!

Agradecimentos
Manoel D. Junior



Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro