Outubro é o Mês de Segurança no Brasil e na América Latina

MÊS de SEGURANÇA

Cibersegurança: como não se tornar vítima ou vilão

Italo Valcy
italovalcy@ufba.br

Créditos

- **Fascículos da Cartilha de Segurança**
  http://cartilha.cert.br/fasciculos/

- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br/

Mas o que é Cibersegurança?

Fonte - http://cartilha.cert.br/

Mas o que é Cibersegurança?

Fonte - http://cartilha.cert.br/

Mas o que é Cibersegurança?

Mas o que é Cibersegurança?

- Segurança da Informação diretamente aplicada no Ciberespaço (“Mundo Digital”)
- O que é Informação?
- Qual o valor da Informação?
- Onde está a informação?

E preciso mesmo me preocupar?

MENU G1 TECNOLOGIA E GAMES

19/08/2011 10h50 - Atualizado em 19/08/2011 10h50

Carregar celular via USB em local público cria risco de roubo de dados

Conexão maliciosa pode roubar dados ou instalar vírus.
Problema foi demonstrado na conferência de segurança Defcon.

G1 - http://goo.gl/GQnUFs

Altieres Rohr
Especial para o G1

Quiosque com carregador de celular: risco de roubo de dados (Foto: Divulgação)

Brian Markus, presidente da Aires Security, e os especialistas Joseph Mlodzianowski e Robert Rowley montaram na conferência de segurança Defcon, em Las Vegas, um quiosque para recarregar gratuitamente a bateria do celular via USB. Ao plugar o celular, no entanto, a tela LCD do quiosque exibia uma mensagem: "você não deve confiar seu smartphone a quiosques públicos. Informação pode ser baixada sem o seu consentimento. Para sua sorte, essa estação é ética e seus dados estão seguros. Aproveite a recarga".

Segundo reportagem do site "Krebs on Security", os especialistas realizaram o experimento para mostrar os riscos de plugar um celular via USB aos participantes da conferência.

A parte mais interessante, diz o texto, foi a reação das pessoas. Um usuário disse "não me importo, pegue meus dados, eu preciso do celular para fazer uma ligação!". Outro apenas conectou o celular, confiante, depois de desativar o modo de transferência USB, mas o celular imediatamente reativou o modo após conectar à estação de carga. "Parece que a configuração não funciona", desabafou.

É improvável que a maioria dos pontos para recarregar a bateria via USB apresente qualquer risco, mas muitos especialistas, mesmo em uma conferência especializada em segurança como a Defcon, nunca pensaram nos riscos de usar conexões USB inseguros para a recarga do aparelho.

Cibercrime brasileiro cria seu primeiro vírus sequestrador

14 Jan 2016 Marvin the Robot Malware, Notícias, Segurança 2 comentários

Por Thiago Marques, pesquisador do GReAT

Não demorou muito para que os cibercriminosos brasileiros começassem a desenvolver suas próprias versões de ransomware com funções de cifragem dos arquivos existentes no computador da vitima. Esta semana encontramos o primeiro virus do tipo desenvolvido no Brasil – o país foi o quarto mais atacado por esse tipo de malware em 2015.

Em meados de 2009, tivemos o caso do Byteclark, que ficou conhecido como o primeiro "Ransomware-like" brasileiro. Porém, ele não possuia nenhuma função de criptografia de arquivos, somente impedia o uso de programas especificos – o que o classificava na verdade como um Blocker.

Fonte - http://cartilha.cert.br/

E preciso mesmo me preocupar?

Implantes podem monitorar tudo que a vítima ouve, vê e diz.

Falha permite que invasor assuma controle de Android com...

Vulnerabilidade JavaScript do navegador Chrome permitiu que pesquisador de segurança assumisse controle de aparelho Ne

idgnow.com.br

Brasiliense sofre golpe financeiro por ter WhatsApp hackeado

Golpista enviou pedidos de transferência bancária urgente a amigos próximos. O desfalque total foi de R$3.500

(Foto: Reprodução)

Google explica vazamento de 5 milhões de senhas do Gmail

Fonte - http://cartilha.cert.br/

E preciso mesmo me preocupar?

- Sequestro de Dados em Laboratório de Pesquisa da UFBA
- Máquina de Raio-X infectada com vírus/malware
- Site da UF*#@/$ infectado e propagando vírus
- Mais de 20 usuários caem em phishing direcionado ao antigo e-mail UFBA (mais de 30 mil spams como consequência)
- Professor perde patente após ter sua pesquisa espionada por grande provedor de e-mail
- Professor teve senha roubada e conta utilizada para envio de mensagens ofensivas em listas institucionais e políticas
- Aluno perde parte de sua dissertação de mestrado ao ter notebook roubado

Fonte - http://cartilha.cert.br/

Códigos Maliciosos

Códigos maliciosos

- **Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos**
- **Também chamados de *malware*, pragas, etc.**
- **Exemplos de equipamentos que podem ser infectados:**
  - **computadores**
  - **equipamentos de rede**
    - ***modems*, *switches*, roteadores**
  - **dispositivos móveis**
    - ***tablets*, celulares, *smartphones***

Códigos maliciosos

- Um equipamento pode ser infectado ou comprometido:
  - pela exploração de vulnerabilidades nos programas instalados
  - pela auto-execução de mídias removíveis infectadas
  - pelo acesso a páginas Web maliciosas, via navegadores vulneráveis
  - pela ação direta de atacantes
  - pela execução de arquivos previamente infectados, obtidos:
    - anexos em mensagens eletrônicas
    - via *links* recebidos por mensagens eletrônicas e redes sociais
    - via mídias removíveis
    - em páginas Web
    - diretamente de outros equipamentos

Códigos maliciosos

- **Porque são desenvolvidos e propagados:**
  - **obtenção de vantagens financeiras**
  - **coleta de informações confidenciais**
  - **desejo de autopromoção**
  - **vandalismo**
  - **extorsão**
- **São usados como intermediários, possibilitam:**
  - **prática de golpes**
  - **realização de ataques**
  - **disseminação de *spam***

Tipos principais

Vírus

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos

- **Depende da execução do programa/arquivo hospedeiro para:**
  - **tornar-se ativo**
  - **dar continuidade ao processo de infecção**
    - **para que o equipamento seja infectado é preciso que um programa já infectado seja executado**
- **Principais meios de propagação: *e-mail* e *pen-drive***

Ransomware (1/2)

Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário

- **Dois tipos principais:**
  - ***Locker*: impede o acesso ao equipamento**
  - ***Crypto*: impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia**

Ransomware (2/2)

- Normalmente usa criptografia forte
- Costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também
- Pagamento do resgate (*ransom*) geralmente feito via *bitcoins*
- Reforça a importância de ter *backups*
  - mesmo pagando o resgate não há garantias de que o acesso será restabelecido

Backdoor

Programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim

Cuidados a serem tomados

Fonte - http://cartilha.cert.br/

Mantenha os equipamentos atualizados

- Use apenas programas originais
- Tenha sempre as versões mais recentes dos programas
- Configure os programas para serem atualizados automaticamente
- Remova:
  - as versões antigas
  - os programas que você não utiliza mais
    - programas não usados tendem a:
      - ser esquecidos
      - ficar com versões antigas e potencialmente vulneráveis

Use mecanismos de proteção

- **Instale um antivírus (*antimalware*)**
  - **mantenha-o atualizado, incluindo o arquivo de assinaturas**
    - **atualize o arquivo de assinaturas pela rede, de preferência diariamente**
  - **configure-o para verificar automaticamente:**
    - **toda e qualquer extensão de arquivo**
    - **arquivos anexados aos *e-mails* e obtidos pela Internet**
    - **discos rígidos e unidades removíveis**
  - **verifique sempre os arquivos recebidos antes de abri-los ou executá-los**

Qual o melhor antivírus?

virustotal

SHA256: f16be42b5ce70190c7a4eba36fad3bbc430f007bb644151f9f0243dd6b664e04

File name: dbc4e20633f6ed966bd2356e425eabb3

Detection ratio: 23 / 55

Analysis date: 2016-10-06 17:16:55 UTC (1 week ago)

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
[illegible]	JS:Trojan.JS.Downloader.FQN	20160930
[illegible]	JS:Trojan.JS.Downloader.FQN	20161006
[illegible]	Trojan/Generic.ASVCS3S.41E	20161006
[illegible]	JS:Trojan.JS.Downloader.FQN	20161006
[illegible]	HEUR/Suspar.Gen	20161006
[illegible]	JS.Trojan-Downloader.Nemucod.lf	20161001
[illegible]	JS:Trojan.JS.Downloader.FQN	20161006

Fonte - http://cartilha.cert.br/

Ao instalar aplicativos de terceiros

- Verifique se as permissões de instalação e execução são coerentes

- Seja cuidadoso ao:
  - permitir que os aplicativos acessem seus dados pessoais
  - selecionar os aplicativos, escolhendo aqueles:
    - bem avaliados
    - com grande quantidade de usuários

Faça *backups* regularmente (1/2)

- Mantenha os *backups* atualizados
  - de acordo com a frequência de alteração dos dados
- Assegure-se de conseguir recuperar seus *backups*
- Mantenha os backups desconectados do sistema (ex: mídia externa)

Seja cuidadoso ao clicar em *links*

- **Antes de clicar em um *link* curto:**
  - **use complementos que permitam visualizar o *link* de destino**
- **Mensagens de conhecidos nem sempre são confiáveis**
  - **o campo de remetente do *e-mail* pode ter sido falsificado, ou**
  - **podem ter sido enviadas de contas falsas ou invadidas**

Fonte - http://cartilha.cert.br/

Segurança em Senhas

Senhas (1/2)

- Servem para autenticar um usuário
  - asseguram que você é realmente quem diz ser, e
  - que possui o direito de acessar o recurso em questão
- Um dos principais mecanismos de autenticação usados na Internet
- Proteger suas senhas é essencial para se prevenir dos riscos envolvidos no uso da Internet:
  - é o segredo das suas senhas que garante a sua identidade, ou seja, que você é o dono das suas contas de usuário

Fonte - http://cartilha.cert.br/

Senhas (2/2)

- **Sua senha pode ser descoberta:**
  - **quando usada em:**
    - **computadores infectados**
    - **computadores invadidos**
    - ***sites* falsos (*phishing*)**
  - **por meio de tentativas de adivinhação**
  - **ao ser capturada enquanto trafega na rede**
  - **por meio do acesso ao arquivo onde foi armazenada**
  - **com o uso de técnicas de engenharia social**
  - **pela observação da movimentação:**
    - **dos seus dedos no teclado**
    - **dos cliques do *mouse* em teclados virtuais**

Senhas

- Senhas fracas
- Informações pessoais
- Somos previsíveis

Confira a lista completa de senhas mais usadas em 2015:

1. 123456	(mesma posição)
2. password	(mesma posição)
3. 12345678	(subiu 1)
4. qwerty	(subiu 1)
5. 12345	(caiu 2)
6. 123456789	(mesma posição)
7. football	(subiu 3)
8. 1234	(caiu 1)
9. 1234567	(subiu 2)
10. baseball	(caiu 2)

Riscos principais

Riscos principais (1/4)

- De posse da sua senha um invasor pode:
  - acessar a sua conta de correio eletrônico e:
    - ler e/ou apagar seus *e-mails*
    - furtar sua lista de contatos e enviar e-*mails* em seu nome
    - enviar mensagens contendo:
      - *spam*
      - boatos
      - *phishing*
      - códigos maliciosos
    - pedir o reenvio de senhas de outras contas
      - e assim conseguir acesso a elas
    - trocar a sua senha
      - dificultando que você acesse novamente a sua conta

Fonte - http://cartilha.cert.br/

Riscos principais (2/4)

- De posse da sua senha um invasor pode:
  - **acessar o seu computador e:**
    - **apagar seus arquivos**
    - **obter informações sensíveis, inclusive outras senhas**
    - **instalar códigos e serviços maliciosos**
    - **usar seu computador para:**
      - **desferir ataques contra outros computadores**
      - **esconder a real identidade desta pessoa (o invasor)**

Riscos principais (4/4)

- De posse da sua senha um invasor pode:
  - acessar a sua conta bancária e:
    - verificar o seu extrato e seu saldo bancário
  - acessar o seu *site* de comércio eletrônico e:
    - alterar informações de cadastro
    - fazer compras em seu nome
    - verificar informações sobre suas compras anteriores
  - acessar o seu dispositivo móvel e:
    - furtar sua lista de contatos e suas mensagens
    - acessar e/ou copiar fotos e vídeos
    - apagar os dados armazenados no dispositivo
  - acessar a sua rede social e:
    - ...

Cuidados a serem tomados

Elaboração de senhas (1/3)

- **Evite usar:**
  - **dados pessoais**
    - **nome, sobrenome**
    - **contas de usuário**
    - **datas**
    - **números de documentos, de telefones ou de placas de carros**
  - **dados disponíveis em redes sociais e páginas *Web***
  - **sequências de teclado**
    - **“1qaz2wsx”, “QwerTAsdfG”**
  - **palavras presentes em listas publicamente conhecidas**
    - **músicas, times de futebol**
    - **personagens de filmes**
    - **dicionários de diferentes idiomas**

Fonte - http://cartilha.cert.br/

Elaboração de senhas (2/3)

- **Use:**
  - **números aleatórios**
    - **quanto mais ao acaso forem os números melhor**
      - **principalmente em sistemas que aceitem exclusivamente caracteres numéricos**
  - **grande quantidade de caracteres**
    - **quanto mais longa for a sua senha melhor**
  - **diferentes tipos de caracteres**
    - **quanto mais "bagunçada" for a sua senha melhor**

Elaboração de senhas (3/3)

- **Dicas práticas para elaborar boas senhas:**
  - **escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra**

    Frase: "Homens de preto qual é sua missão?"

    Senha: "?HdpQehSm15540"
  - **escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres**

    Senha: "1 dia ainda verei os aneis de Saturno!!!"
  - **invente um padrão de substituição próprio**

    Padrão: substituir "o" por "0" e duplicar as letras "s" e "r"

    Frase: "Sol, astro-rei do Sistema Solar"

    Senha: "SS0l, asstrr0-rrei d0 SSisstema SS0larr"

Uso de senhas (3/3)

- **Crie grupos de senhas, de acordo com o risco envolvido:**
  - **crie senhas:**
    - **únicas, fortes, e use-as onde haja recursos valiosos envolvidos**
    - **únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior**
    - **simples e reutilize-as para acessos sem risco**

- **Armazene suas senhas de forma segura:**
  - **anote-as em um papel e guarde-o em local seguro**
  - **grave-as em um arquivo criptografado**
  - **use programas gerenciadores de contas/senhas**

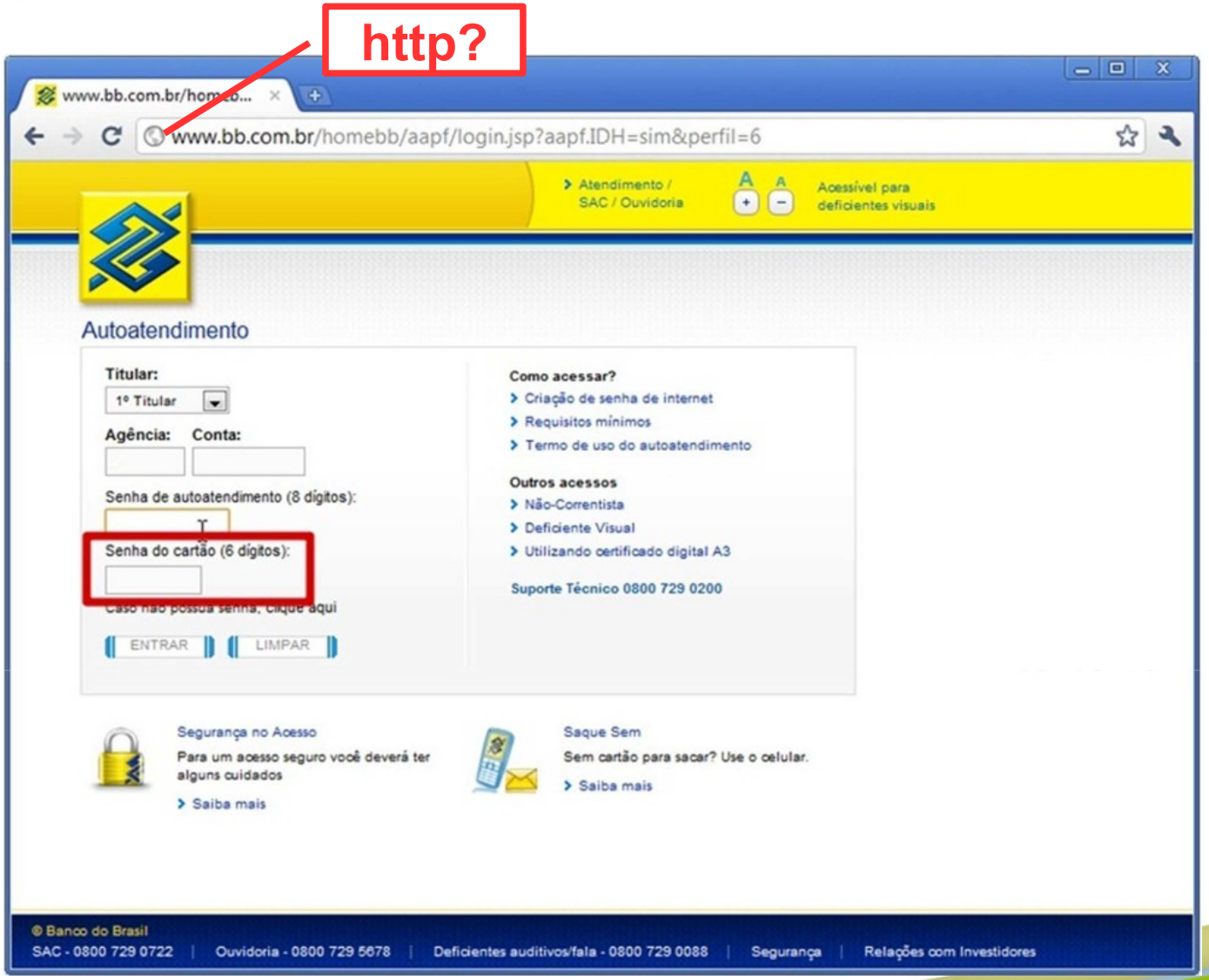
Alteração de senhas

- **Altere suas senhas:**
  - **imediatamente, se desconfiar que elas tenham sido:**
    - **descobertas ou usadas em computadores invadidos ou infectados**
  - **rapidamente:**
    - **se perder um computador onde elas estejam gravadas**
    - **se usar uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles**
  - **regularmente:**
    - **nos demais casos**

Phishing e códigos maliciosos

- **Desconfie de mensagens recebidas:**
  - **mesmo que enviadas por conhecidos**
- **Evite:**
  - **clicar/seguir *links* recebidos via mensagens eletrônicas**
- **Seja cuidadoso ao acessar *links* reduzidos:**
  - **use complementos que permitam expandir o *link* antes de clicar sobre ele**

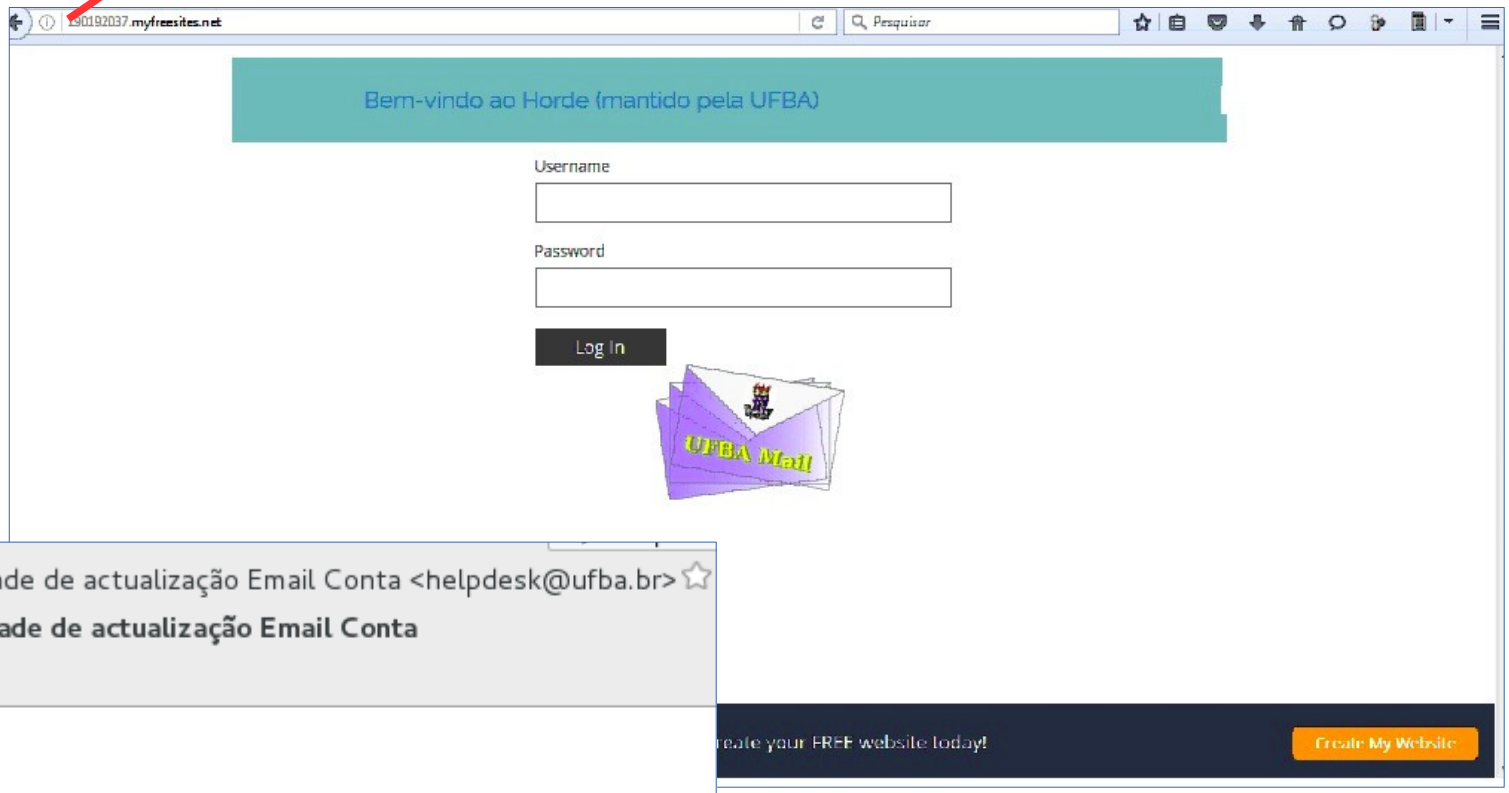
Phishing e códigos maliciosos



Fonte - http://cartilha.cert.br/

Phishing e códigos maliciosos

http://190192037.myfreesites.net



De Universidade de actualização Email Conta <helpdesk@ufba.br>

Assunto **Universidade de actualização Email Conta**

Para

--
Atenção
Estamos actualmente a fazer o processo de manutenção de todos os e-ma
imediatamente a este e-mail, para verificar sua conta contra spyware
seguindo os links.

Para atualizar, clique aqui
http://190192037.myfreesites.net/

Fonte - http://cartilha.cert.br/

Cuidados ao se conectar a redes Wi-Fi

Wi-Fi – Cuidados ao conectar

- **Não permita que seus dispositivos conectem-se automaticamente:**
  - **a redes públicas**
  - **a redes que você já tenha visitado**
    - **um criminoso pode configurar uma rede com o mesmo nome de uma rede já utilizada por você**
    - **sem saber você estará acessando essa rede falsa**

- **Lembre-se de apagar as redes que você visitou**
  - **isso ajuda a preservar a sua privacidade**

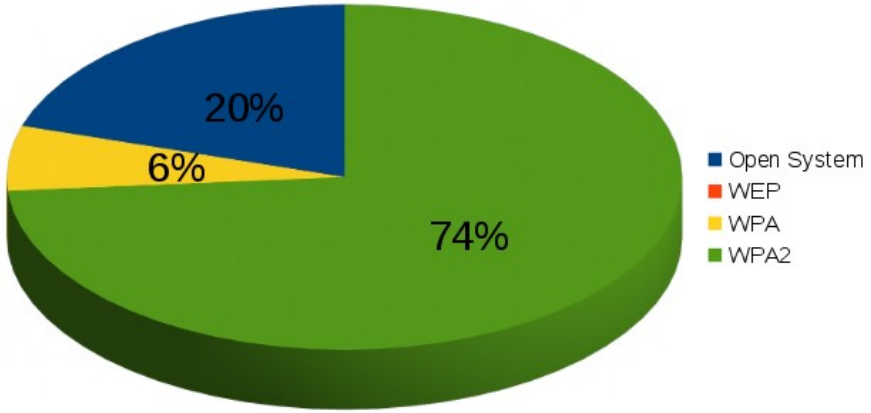
Wi-Fi – Cuidados ao conectar

- **Redes com Portal de Autenticação apenas não implicam em maior segurança**

- **Procure usar redes que ofereçam criptografia WPA2**
  - **evite usar WEP e WPA**

Wi-Fi na UFBA

Qual nível de segurança das redes Wi-Fi?



Wi-Fi na UFBA

- Em pesquisa recente foram identificadas mais de 100 redes Wi-Fi no campus de Ondina
  - Problemas de qualidade
  - Muitos dispositivos com redes no padrão de fábrica
  - Problemas de segurança
- Uso massivo da rede UFBA-Visitante, sem criptografia
- Utilizem a rede “eduroam”!

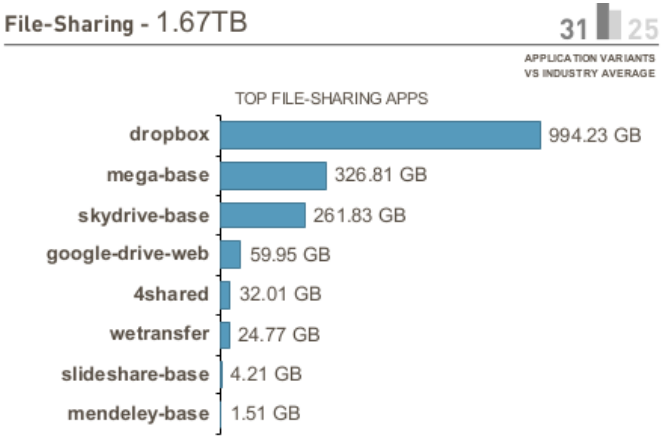
Serviços de Nuvem e Privacidade

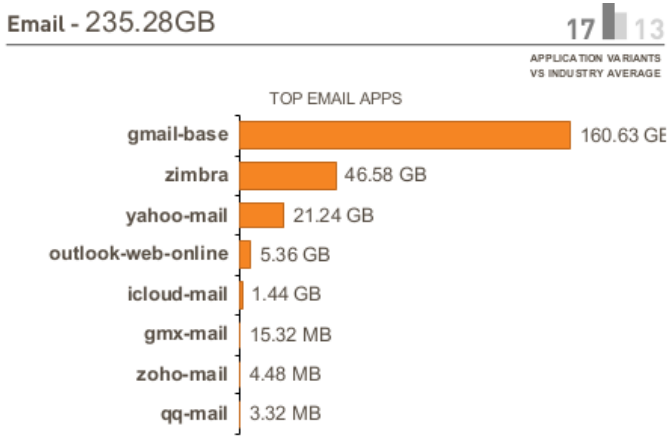
Uso de nuvem pública

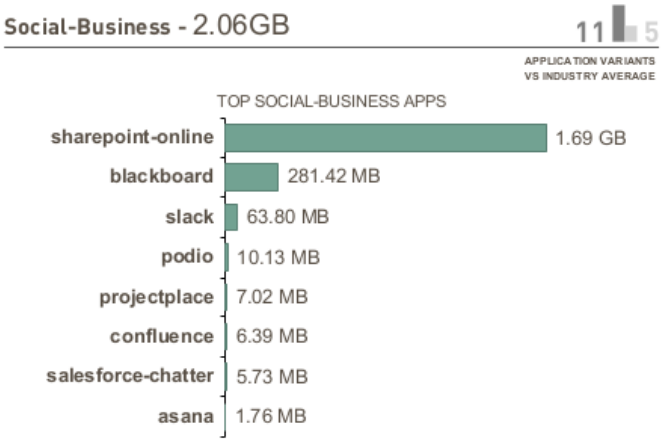
- Muitas funcionalidades, muito espaço, acesso de qualquer lugar, serviços “gratuitos”
- A comunidade UFBA faz uso massivo de serviços de nuvem pública
  - Ferramentas de compartilhamento de arquivo
  - Ferramentas de escritório
  - E-mail
  - Redes sociais, IM, audio/vídeo

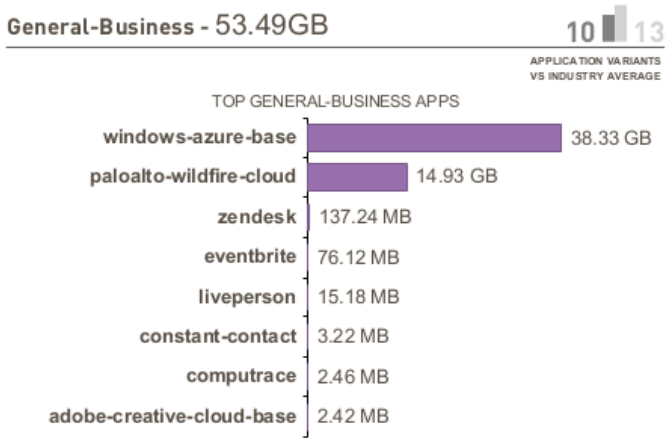
Fonte - http://cartilha.cert.br/

Uso de nuvem pública









Fonte - http://cartilha.cert.br/

Termos de uso dos serviços

- **Exemplo: Google**

Quando você faz upload, submete, armazena, envia ou recebe conteúdo a nossos Serviços ou por meio deles, você concede ao Google (e àqueles com quem trabalhamos) uma licença mundial para usar, hospedar, armazenar, reproduzir, modificar, criar obras derivadas (...) para os fins restritos de operação, promoção e melhoria de nossos Serviços e de desenvolver novos Serviços. Essa licença perdura mesmo que você deixe de usar nossos Serviços (…). Certifique-se de que você tem os direitos necessários para nos conceder a licença de qualquer conteúdo que você enviar a nossos Serviços.

Fonte - http://cartilha.cert.br/

Cuidados

- Evite disponibilizar dados pessoais de forma irrestrita nos serviços de nuvem
- Utilize criptografia (LUKS, TrueCrypt, VeraCrypt)
- Atente-se para os termos de uso

- … Utilize com moderação!

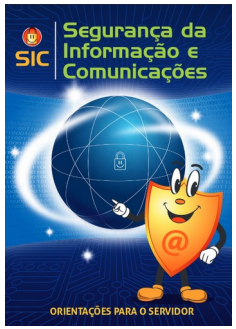
Em resumo

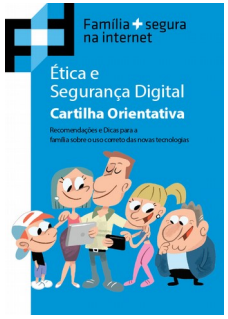
- É importante ter cuidados básicos no uso de recursos de Tecnologia da Informação
- Procure orientações e apoio técnico de especialistas
- Desconfie sempre (solicitação de dados, mensagens e arquivos suspeitos, etc), mas sem paranóia!
- Ao encontrar problemas ou crimes cibernéticos, denuncie!
  - http://new.safernet.org.br/denuncie
  - ETIR/UFBA <etir@ufba.br>

Mantenha-se informado (1/3)

Cartilhas de Segurança na Internet

https://gsic.ufba.br/outras-cartilhas





Fonte - http://cartilha.cert.br/

Mantenha-se informado (2/3)

Safernet

http://www.safernet.org.br/

Portal Internet Segura

http://www.internetsegura.br/

Mantenha-se informado (2/2)

Campanha Internet Sem Vacilo

http://internetsemvacilo.org.br/

Obrigado pela atenção! Dúvidas?

Gestão de SIC/UFBA <gsic@ufba.br>

https://gsic.ufba.br/meseg