(In)Segurança Virtual

Introdução

Expotec 2009 – IFRN- Campus Mossoró

Eliakim Aquino - eliakim_pcdoctor@hotmail.com

interseguraca.blogspot.com

Mossoró-RN
Setembro-2009

Que idéia seria essa?

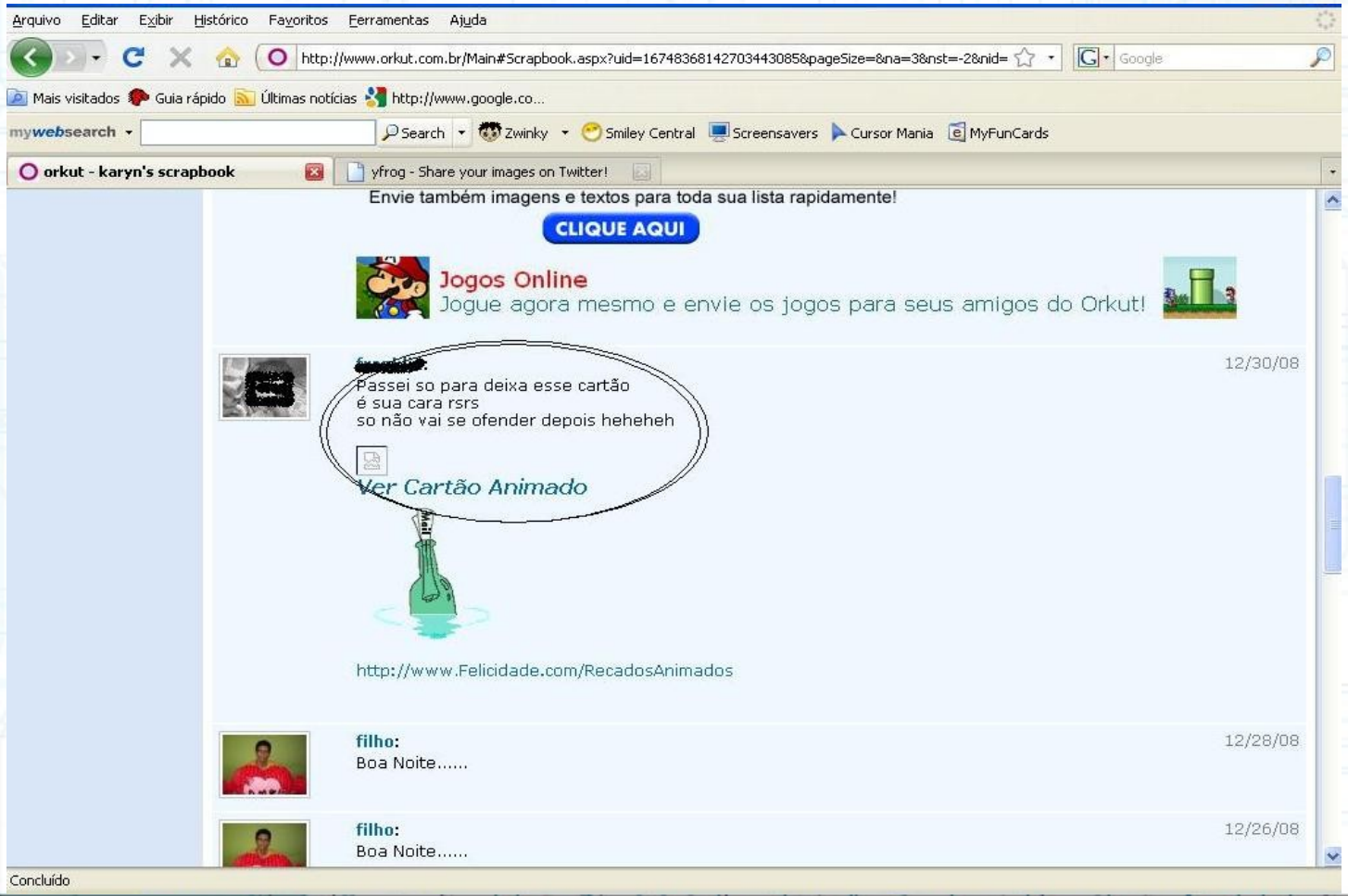
- Fator Humano: O elo mais fraco da segurança:

“Apenas duas coisas são infinitas: O universo e a estupidez humana, e ainda não estou certo sobre a primeira.”

Albert Einstein

O elo da segunrança

- As pessoas entram no mundo virtual totalmente despreparadas, tanto para operar um computador ou prover segurança básica no PC.



O elo da segurança

- A resposta é simples. Embora a pessoa seja realmente um adulto, na internet é como se ela fosse um criança.
- Todas as pessoas que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadadas a sofrer da ilusão da segurança.

Antivírus

- Qual o melhor antivírus?
  - O melhor antivírus é aquele que está sentando entre a cadeira e o monitor!
  - A segurança não é um produto, ela é um processo!

Hacker, o que é isso?

- **Guru:** Grau máximo na hierarquia. Um exemplo de guru é o Linus Torvalds, criador do Linux.
- **Hacker:** Especialista em burlar a segurança de sistemas informatizados.
- **Phreaker:** Especialista em burlar sistemas de telefonia, foi uma das primeiras formas de hacking.
- **Cracker:** Especialista na quebra de senhas de programas. No Brasil está definição está sendo usado para definir o hacker que comete crimes.
- **Script Kiddie:** Não é iniciante, mas não sabe o suficiente para ser considerado um hacker. Usa o que sabe pra fazer pequenos delitos e perturbar os usuários de internet.
- **Lamer:** O iniciante que costuma fazer papel de bobo ao tentar dar passos maiores que as pernas.

Como surgiram os Hacker?

- No inicio dos anos 60 programadores do MIT se auto-intitularam “hackers”. O termo hacker naquela época era usado pra definir alguém muito bom no que fazia. Se o significado original não fosse desvirtuado, hoje teríamos hackers em diversas profissões.
- Neste sentido, os hackers foram os que criaram e mantém a internet funcionando.
- Na década de 80 surgiram os primeiros vírus populares e as primeiras ações hackers feitas por grupos.
- Nos anos seguintes, a imprensa, o cinema e os escritores, acabaram por vincular definitivamente a palavra hacker com computadores e crimes de informática.

Mente Hacker

- A mente Hacker é uma mente sem medo, enfrenta o grande sabendo que ele é fraco, Descobre a falha no impecável. Derruba paredes soltando um único tijolo. Pensa no obvio, mas que ninguém pensou antes. Descobre caminhos novos nas mesmas passagens. Incomoda por mostrar que as coisas não são o que parecem.

Mente Hacker

Hacker: “Do que você tem medo?”

Usuário Comum: *“Não é bem medo.”*

Hacker: “É o que então?”

Usuário Comum: *“Na verdade eu não sei. Talvez uma precaução. Eu não quero que um hacker me faça mal.”*

Hacker: “Que tipo de mal?

Usuário Comum: *“Sei lá. Ler meus emails por exemplo.”*

Hacker: “E tem muita coisa importante em seu email? Digo coisas importantes para um hacker”?

Usuário Comum: *“Não são coisas tão importantes assim. Mas eu quero a minha privacidade.”*

Mente Hacker

Hacker: “E este monte de câmeras no meio da rua? Nós fomos filmados no Santo Dumont e seremos filmados em Congonhas e seremos filmados o tempo todo nas ruas e prédios de São Paulo. Você ainda acha que tem privacidade em um grande centro?”

Usuário Comum: *“E se um hacker invadir o meu micro?”*

Hacker: “Eu devolvo a pergunta e se um hacker invadir o seu micro? O que tem de importante para um hacker lá?”

Usuário Comum: *“Minhas coisas.”*

Hacker: “Posso saber que coisas são estas?”

Usuário Comum: *“Têm minhas músicas, jogos, umas gatas. Você sabe...”*

Hacker: “Na verdade eu não sei. Só acho que, embora para você tenha valor um monte de músicas pirata, jogos e fotos de mulher pelada, não consigo ver como um hacker usaria estas coisas para te fazer mal? Se fosse pelo menos um Paulo Coelho com os originais do seu próximo livro eu até entenderia a preocupação. Mas isto que você guarda... Sinceramente.”

O seu verdadeiro inimigo

- Seu verdadeiro inimigo está mas próximo do que você imagina!

Engenharia Social

- O elemento mais vulnerável de qualquer sistema de segurança da informação é o **ser humano**, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social. Dentre essas características, pode-se destacar:
  - **Vaidade pessoal e/ou profissional.**
  - **Autoconfiança.**
  - **Formação profissional.**
  - **Vontade de ser útil.**
  - **Busca por novas amizades.**
  - **Propagação de responsabilidade.**
  - **Persuasão.**

A queda da rede

- A primeira ligação: Marcos Augusto Marcos Augusto, Contabilidade.“
  - “Marcos, aqui é Eddie Martin do Help Desk. Estamos tentando solucionar um problema de rede de um computador. Você sabe se alguém do seu grupo vêm tendo problemas para permanecer conectado?"
  - "Hum, não que eu saiba."
  - "E você não está tendo problemas?"
  - "Não, tudo parece bem."

- "Bem, isso é bom. Ouça, estamos ligando para as pessoas que podem ser afetadas, por

  isso é Importante que você nos informe imediatamente se perder a sua conexão

  de rede."
- "Isso não parece bom. Você acha que pode acontecer?"
- "Esperamos que não, mas você liga se acontecer alguma coisa, certo?"
- "Pode acreditar que sim."
- "Ouça, parece que ficar sem a conexão de rede é problema para você..."
- "Pode apostar que seria.“
- "...então enquanto estamos falando disso, vou dar o número do meu telefone celular. Se

  precisar, você pode ligar direto para mim."
- "Isso seria ótimo."
- "O número é 555-867-5309."
- "555-867-5309. Entendi, obrigado. Qual é mesmo o seu nome?"

- "É Eddie. Mais uma coisa, preciso verificar o número de porta ao qual o seu computador

  está conectado. Dê uma olhada no seu computador *e veja se há uma etiqueta em*

  algum lugar dizendo algo como 'Número de porta'."
- "Espere um pouco... Não. não vejo nada parecido."
- "OK, então na parte de trás do computador você consegue reconhecer o cabo de rede?"
- "Sim."
- "Veja onde ele está ligado. Veja se há uma etiqueta no conector ao qual ele está

  Ligado.
- "Espere um pouco. Sim, espere aí, tenho de me ajoelhar para chegar mais perto e ler,

  Muito bem, é a porta 6 traço 47."
- "Bom, é isso o que tínhamos, só queria ter certeza,"

- A segunda ligação: O cara de TI
  - Dois dias depois, uma ligação foi recebida no Centro de Operações de Rede da mesma

    empresa.
  - "Olá, aqui é Bob. Trabalho na Contabilidade do escritório de Marcos Augusto. Estamos
  - tentando solucionar um problema de cabo. Preciso desativar a Porta 6-47."
  - O rapaz de TI disse que isso seria feito em alguns minutos e pediu que eles avisassem

    quando poderiam ativar novamente a porta.

- "É, temos um monte de gente assim agora. Até o final do dia tudo estará resolvido. Tudo

  bem?"
- "NÃO! Droga, vou me atrasar muito se tiver de esperar tanto. Qual é o melhor prazo que

  você tem para mim?"
- "Qual é a sua urgência?"
- "Posso fazer outras coisas agora. Há alguma chance de você consertar isso em meia

  hora?"
- "MEIA HORA! Você não está querendo muito? Bem, vejamos, vou parar o que estou

  fazendo e ver se consigo resolver isso para você."
- "Olha, obrigado mesmo, Eddie.“

- A quarta ligação: você conseguiu!
  - Quarenta e cinco minutos depois...
  - Marcos? Aqui é o Eddie. Tente se conectar na rede agora.". Após alguns momentos:
  - "Ah, que bom está funcionando. Isso é ótimo.""Bom, estou feliz que consegui cuidar disso para você."
  - "Sim, muito obrigado."
  - "Ouça. se quiser ter certeza de que a sua conexão não vai cair novamente, você precisa

    executar alguns softwares. Isso só vai levar uns minutos."
  - "Mas agora não é uma hora boa."
  - "Entendo... Mas isso poderia evitar grandes dores de cabeça para nós dois da próxima

    vez que esse problema de rede acontecesse de novo."
  - "Bom... se são apenas alguns minutos."
  - "Faça o seguinte..."

- Eddie instruiu Tom para fazer o download de um pequeno aplicativo de um site Web.
- Após o programa ser carregado. Eddie disse a Tom para clicar duas vezes nele. Ele

  tentou, mas disse:
- "Não está funcionando. Não está acontecendo nada."
- "Ah. que pena. Deve haver algo de errado com o programa. Vamos nos livrar dele.
- podemos tentar novamente outra hora." E instruiu Tom para excluir o programa de
- modo que ele não pudesse ser recuperado.