SEGURANÇA NA INTERNET

08.10.2015

Sugestões e ferramentas para nos proteger na utilização deste meio de comunicação universal.

Segurança na Internet

- **A Internet é, sem dúvida, o mais bem sucedido meio de comunicação , uma vez que nos abre as portas da informação global, de uma forma que não sonharíamos há alguns anos atrás.**

Fatos sobre a Internet

- A Internet propaga e perpetua;
- A informação corre o mundo em menos de "um segundo";
- Uma foto nunca mais será apagada;
- A informação que se apresenta não tem filtros, por vezes a informação que nos chega, não é tratada, não contextualizada, levando a erros de interpretação.

Alguns Perigos da utilização da internet

- Cyberbulling;
- Jogos de apostas On-line;
- Acesso ilegal de sites e conteúdos;
- Falso anonimato (fake);
- Contato com pessoas mal-intencionada;
- Conteúdo ilegal (músicas, filmes ..);
- Racismo e Preconceito;
- Calúnia e Difamação (Utilização de nomes falsos);
- Dependência;
- Pornografia e Pedofilia – conteúdo fácil de aceder;

Segurança na Internet

Antigamente: “Não aceites doces de estranhos na rua!”

Hoje: “ Não divulgue dados pessoais na rede! ”

Técnicas de ataque

- Engenharia Social - Esta técnica compreende em obter informações, por parte dos utilizadores por correio eletrónico, por telefone, ou por contacto direto.
- Phishing;
- Malware / Programas Maliciosos;
- Ataques a vulnerabilidades dos sistemas operativos;

Técnicas de ataque – Engenharia social

- Alterar a sua identidade, para fins ilícitos, um exemplo flagrante são os casos de pedofilia;

http://www2.fcsh.unl.pt/eukidsonline/docs/NavSegNaInternet_PEDOFILIA.pdf

http://www.publico.pt/destaque/jornal/o-mundo-escorregadio-da-pedofilia-na-internet-198150

Nos primeiros setes meses de 2014 a policia Judiciaria apanhou 93 pedófilos dos quais 24 ficaram presos preventivamente.

http://www.asjp.pt/2014/09/03/93-pedofilos-apanhados-em-sete-meses/

- O caso da wikileaks ;
- O caso da Pepsi e a Coca-Cola; " Um técnico de som transferiu informação confidencial /estratégica da Pepsi para a Coca-Cola "

Mais exemplos:

https://www.trustsign.com.br/portal/blog/6-casos-reais-de-falhas-de-seguranca-em-grandes-empresas/

Técnicas de ataque Cyberbulling

- Os agressores aproveitam, por exemplo, as fotos das vítimas para difamarem a sua imagem, ou o e-mail, facebook, twitter ...

Em 1000 raparigas dos 10 aos 18 Anos , 28% já foram vitimas de cyberbulling.

É necessário estar atento aos sinais;

Psicologicamente o bullying é devastador, conduzindo a consequências muito graves.

- As agressões não têm um rosto, muitas vezes partem de um perfil /email anonimo, a sua propagação é muito rápida a atinge um população muito vasta.

http://pplware.sapo.pt/informacao/cyberbullying-o-que-como-combater/

http://cyberbullying.org/

http://cyberbullyingportugal.blogspot.pt/

Técnicas de ataque Malware / Virus

Programas maliciosos

- "pela exploração de vulnerabilidades existentes nos programas instalados;
- Pela auto-execução de unidades amoviveis infectadas (*pen-drives, discos, cartões de memória)* ;
- Pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- Pela ação direta de quem ataca, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- Pela execução de arquivos previamente infectados, obtidos em anexos de e-mails, em páginas *Web* ou diretamente de outros computadores (através da partilha de recursos).

Técnicas de ataque Malware / Virus

- Regista todas a teclas que o utilizador está a utilizar;

  Password's, textos, conversas ….

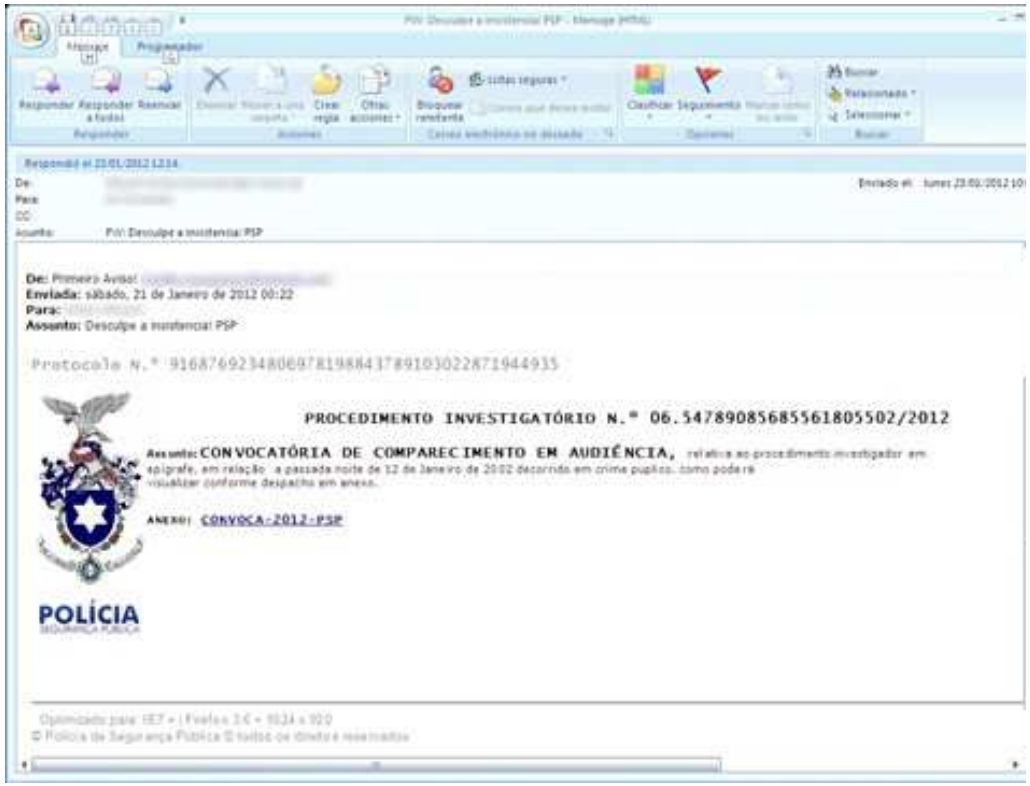
- Utilizar o computador infetado, para atacar outros;

- Tomar conta do computador, obtendo acesso a informação que se encontra no disco rígido.

Técnicas de ataque Malware / Virus

Ao abrir o ficheiro que está anexo ao e-mail, o destinatário está "automaticamente a ativar um programa destinado a recolher todos os dados do computador“

http://www.jn.pt/PaginaInicial/Tecnologia/Interior.aspx?content_id=2266013



Técnicas de ataque Malware / Vírus

- Programas maliciosos

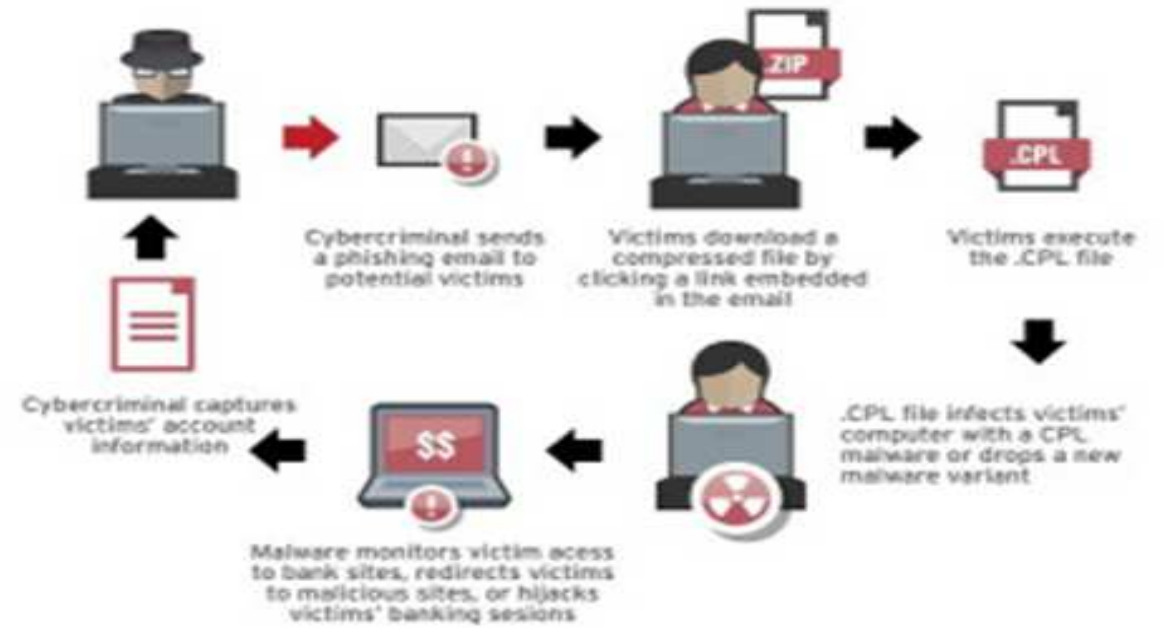
"O ano de 2012 foi um ano de grandes perigos para todos os utilizadores que deram uso a plataformas de jogo online. A área do gaming está a atrair a atenção dos piratas informáticos pelos vários tipos de bens que podem ser roubados. A comprovar a situação estão os sete mil ataques maliciosos diários feitos contra *gamers*, o que totaliza cerca de 2,55 milhões de tentativas de hacking durante o último ano.

Roubo de credenciais de acesso aos jogos para sequestro de contas e venda de itens ou até das personagens a troco de dinheiro real, e roubo de informações pessoais que incluem palavras-chave de acesso a contas bancárias, são as principais razões que movem os cibercriminosos.

http://tek.sapo.pt/noticias/internet/artigo/jogadores_online_alvo_de_2_55_milhoes_de_ataques_maliciosos_em_2012-1303699tek.html

Técnicas de ataque – Mawlware / Virus

Esquema de Ataque



Técnicas de ataque – Mawlware / Virus

Caso de um Link que nos leva para um download de uma aplicação

Técnicas de ataque – Mawlware / Vírus

- Caso CNN e vírus Ébola

http://noticias.softonic.com.br/ataques-virtuais-virus-ebola-para-atrair-usuario-a-golpes-online

- Caso de um e-mail supostamente do youtube

Técnicas de ataque – Phishing

- Geralmente chega às pessoas via e-mail.
- Envio de e-mail's provenientes de instituições conhecidas.

Bancos, Forças de segurança, CTT …

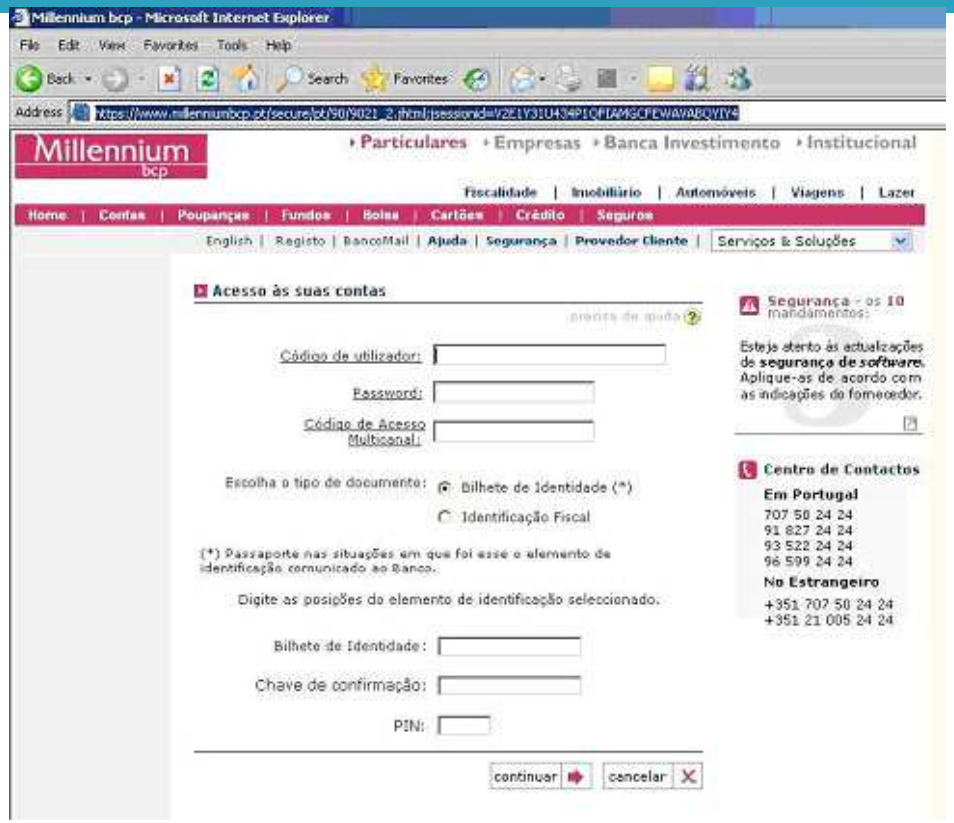
solicitam numero de cartões de crédito, N° De contas Bancárias, telefones, moradas, códigos de segurança etc.

Técnicas de ataque – Phishing

Técnicas de ataque – Phishing /Malware

Trata-se de um software malicioso instalado no computador, que tem a capacidade de manipular as páginas apresentadas pelo Browser

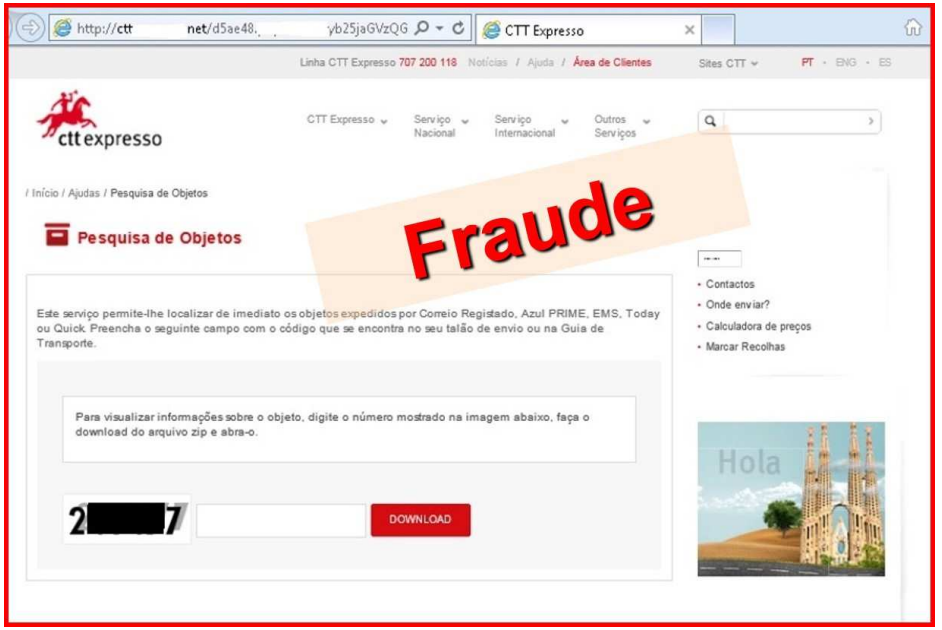
http://ind.millenniumbcp.pt/pt/Particulares/seguranca/Pages/Phishing.aspx



Técnicas de ataque – Phishing

Caso dos CTT

Neste exemplo são e-mail's enviados com link fraudulento e que têm como intuito a recolha ilícita de credenciais pessoais associadas a contas de e-mail ou a outros serviços online.



Técnicas de ataque – Phishing

A mesma imagem da CGD Mas não é verdadeira,

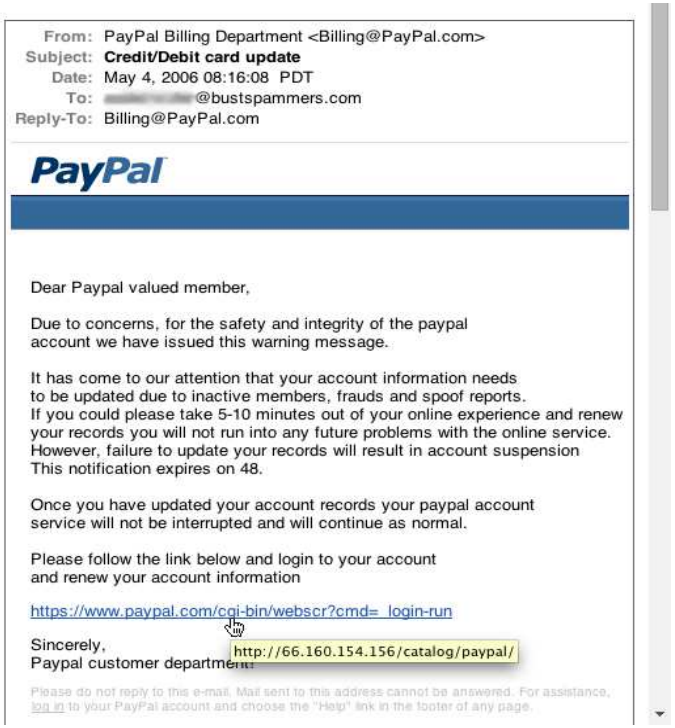
O link não aponta para o site oficial

Técnicas de ataque – Phishing

O link está errado, tem um s que não devia ter, mas que passa despercebido.

Http://www.gruposantanders.es/

No exemplo do paypal – O link aponta para um endereço que não é o mesmo que se encontra descrito. Ainda por cima, trata-se de um endereço numérico direto, não é normal.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]@bustspammers.com
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

Técnicas de Proteção

"A melhor maneira de ficar em segurança é nunca se sentir seguro."
(Benjamin Franklin)

Procedimentos de segurança

- Estar sempre à defesa, quando recebe qualquer conteúdo ou quando visita um determinada página que não conhece;
- Aceitar e-mail's e informação de quem é apenas conhecido, mesmo assim, quando o conteúdo não seja simples deverá desconfiar;
- Ter cuidado ao abrir imagens ou anexos de e-mail;

Procedimentos de Segurança

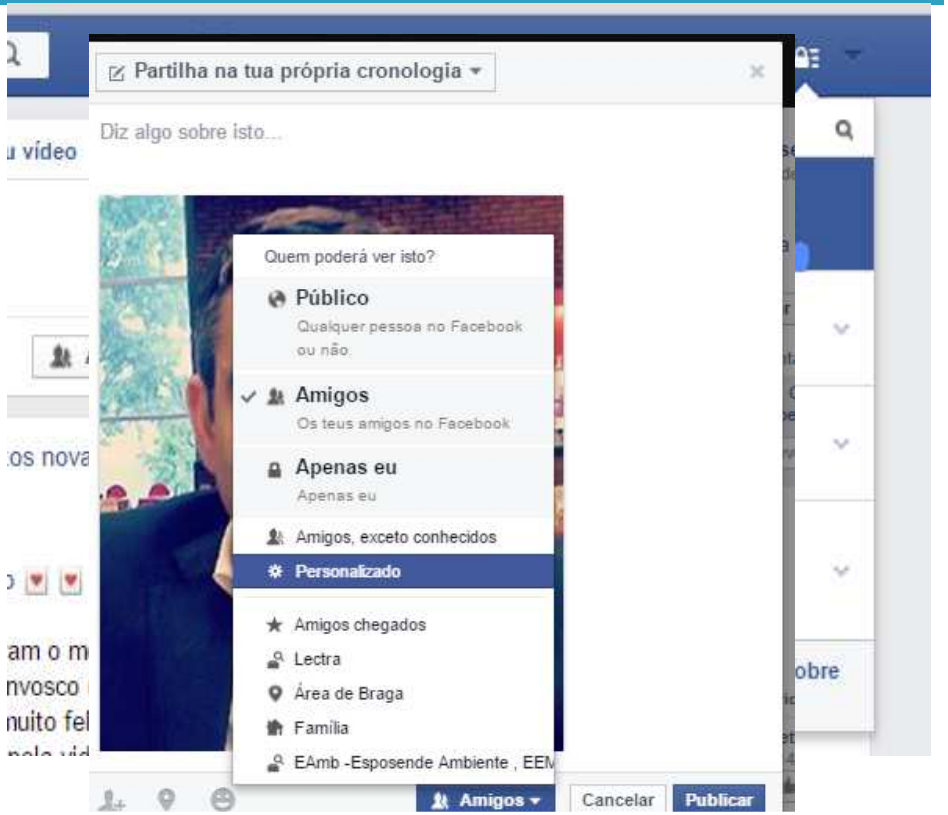
- No Facebook ou redes sociais:

  - Aceitar pedidos de amizade realmente de quem se conhece;

  - Utilizar as ferramentas de privacidade;

  - Evitar a publicação de fotos pessoais em modo publico;

  - Estudar bem os perfis que pretendem contactar;



Procedimentos de Segurança

- Manter os Antivírus / aplicações de Malware e Spyware atualizados:

  Exemplos de distribuições gratuitas:

  - AVG http://free.avg.com/pt-pt/homepage ;
  - AVAST https://www.avast.com/pt-pt/index ;
  - MalwareBytes https://www.malwarebytes.org ;

- Manter os sistemas operativos atualizados e respetivas aplicações de suporte, ativar as atualizações automáticas

Procedimentos de Segurança

- Não confie em janelas pop-up que solicitam que você faça o download de um software;
- Tenha atenção aos falsos alertas de vírus ;
- Alterar as password's regularmente ou se considera que a atual, possa estar comprometida;

Informação Útil

http://www.internetsegura.pt/

https://linhaalerta.internetsegura.pt/

http://cartilha.cert.br/




Obrigado

José António Fernandes

jose.antonio@esposendeambiente