**Segurança em:**

**Dispositivos moveis**

Assim como os computadores os dispositivos moveis podem ser usados para praticas maliciosas como furto de dados, envio de spam, propagação de códigos maliciosos, e pode fazer parte de botnets usado para disparar ataques a internet.

Os cuidados com os dispositivos moveis são os mesmos que tomamos com os computadores pessoais, como manter sempre atualizado e utilizar mecanismos de segurança (antivírus).

**IoT (Internet of Things)**

A internet das coisas são infraestruturas de redes dinâmicas globais, para se ter segurança e um ambiente IoT é preciso conciliar as prioridades de TI (tecnologia da informação) que é voltada para segurança da informação e de OT (tecnologia operacional) que é responsável por gerir redes de controle que suportem a infraestrutura crítica e os espaços físicos. Ao trabalhar em conjunto a segurança pode ser aplicada em toda a rede IoT considerando três abordagens, visibilidade em tempo real, consciência da ameaça, e ações quando são identificadas as ameaças.

**Operações bancárias e comerciais**

Com o avanço da internet e dos dispositivos moveis, está cada vez mais comum fazer operações bancarias ou comerciais sem sair de casa, sem ter que ir a uma loja física, e como toda evolução esta também tem seu lado positivo e negativo. É preciso tomar algumas medidas basicas para se ter segurança neste tipo de operação:

* Antivírus atualizado
* Realizar transações em sites confiáveis
* Verificar se o endereço apresentado é o que quer acessar
* Não realizar transações me computadores públicos

**Senhas seguras**

Hoje a segurança é mais importante que nunca. Com o aumento de transações online, redes sociais, e transferência de arquivos corporativos por e-mail, uma boa senha é essencial. Softwares desenvolvidos para invasão são de fácil acesso para todos. Com o uso da engenharia social, crackers aproveitam da ingenuidade de pessoas para a invasão e roubo de dados.

É simples se proteger: evitar datas importantes, iniciais do nome, nome de animais, parentes, ou hobbies, procurar usar letras e números, maiúsculas e minúsculas. Ás vezes danos morais não são levados a sério, contrário disso os danos financeiros são mais temidos.

**1 - Cybersecurity**

É um termo que usamos para proteção de computadores, redes, programas e dados contra o acesso não autorizado, ou alteração e destruição dos mesmos. Está cada vez mais comum noticias sobre informações sigilosas roubadas e publicadas na internet.

Existe três aspectos importantes na cybersecurity:

* integridade
* confidencialidade
* disponibilidade

**A importância do Cybersecurity**

Governos, militares, corporações, instituições financeiras, hospitais, dentre outras organizações recolhem, armazenam, e processam uma grande quantidade de informações sigilosas em seus computadores, e transmitem esses dados através da rede para vários lugares do mundo. Como os ataques vêm crescendo e ficando cada vez mais sofisticados é preciso atenção continua para proteger esses dados importantes.

**O que fazer para evitar**

O setor da tecnologia da informação precisa estar bem preparado, investir em praticas modernas de segurança, como antivírus conceituado, firewall com recursos de ultima geração, investir em políticas de segurança da informação.

**2 - Cybercrime**

São crimes cibernéticos que envolva qualquer atividade ou pratica ilícita na rede. Como por exemplo invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações pessoais entre outros. O cybercrime compreende também crimes realizados por meio de dispositivos eletrônicos ou qualquer ação digital para praticar crime.

Principais crimes cibernéticos:

* Pornografia infantil
* Lavagem de dinheiro
* Ciberterrorismo
* Ciberativismo
* Roubo

**O que fazer para evitar**

Não abrir email com anexo suspeito vindo de pessoas desconhecidas e também desconfiar de email de ofertas, evitar sites pouco conhecidos ou com conteúdo duvidoso. Manter o antivírus e o firewall ativo e atualizado.

**3 - Cyberwar**

É um conflito que não ocorre com armas físicas, ocorre através da confrontação com meios eletrônicos e informáticos no chamado ciberespaço, no intuito de enfraquecer e retirar do ar serviços de internet, sistemas água e energia, e propagar vírus e mensagens maliciosas. É um ataque cibernético feito por uma pessoa, grupo de pessoas ou organizações, que visam derrubar um inimigo por situação conflito, político-ideológico, financeiro ou religioso.

**Quem são os alvos**

Qualquer setor importante para a infraestrutura do inimigo, por exemplo exército, defesa nacional, indústria bélica. Em uma versão mais assustadora a cyberguerra pode ter como alvo o recurso mais importante do pais que é sua população. Um hacker poderia fazer um ataque terrorista para desestabilizar ou desmotivar uma população a lutar. Isso implica em coisas assustadoras como ataques aos setores financeiros, que causariam danos econômicos; ou ataques a sistemas de comunicação – imagine o que aconteceria se a rede de telefonia fosse desativada e a internet caísse.

**3 – Cyberspionage**

Desde o inicio da internet a cyberspionage vem sendo praticada e hoje em dia vem sendo usada por algumas corporações como polícia e serviço secreto governamentais. Cyberspionage consiste em obter informações sigilosas de terceiros sem a permissão do titular da informação com técnicas de hacking ou cracking.

**Quem são os alvos**

Competidores, rivais, grupos e inimigos por vantagem pessoal, econômica, política, militar. Os eventos mais conhecidos de espionagem que chegou ao público foram a “Ghostnet” e “Outubro Vermelho”. Ghosnet se infiltrou em 1295 computadores em 103 paises, Outubro Vermelho foi uma campanha avançada de cyberspionage dirigida as organizações diplomáticas e centros de investigações cientificas, e governos de todo o mundo.

**Referencias**

CYBER SECURITY – COMO CUIDAR DESTE TEMA

[www.afrikatec.com.br/cyber-security-como-cuidar-deste-tema/](http://www.afrikatec.com.br/cyber-security-como-cuidar-deste-tema/)

SEGURANÇA DE COMPUTADORES

<https://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_computadores>

O QUE É CIBERCRIME

<https://canaltech.com.br/seguranca/O-que-e-cibercrime/>

CRIME INFORMATICO

<https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>

CIBERGUERRA

<https://pt.wikipedia.org/wiki/Ciberguerra>

O QUE É CIBERGUERRA

<http://amadodosenhor.comunidades.net/o-que-e-ciberguerra>

CYBER SPYING

<https://en.wikipedia.org/wiki/Cyber_spying>

CIBERSPIONAGEM GLOBAL E O DECRETO 8.135: UMA AVALIAÇÃO SEGURANÇA DAS INFORMAÇÕES DO GOVERNO BRASILEIRO

<https://pt.slideshare.net/mvsecurity/artigo-consad-2014-ciberespionagem-global-e-o-decreto-8135-uma-avaliao-da-segurana-das-informaes-do-governo-brasileiro>

OS DESAFIOS EM SEGURANÇA DIGITAL COM A INTERNET DAS COISAS

http://www.techmag.com.br/novidades/os-desafios-em-seguranca-digital-com-a-internet-das-coisas/

INTERNET DAS COISAS E SEGURANÇA DA INFORMAÇAO

<https://www2.deloitte.com/br/pt/pages/risk/articles/impacto-da-iot.html>

SEGURANÇA EM OPERAÇOES BANCARIAS VIA INTERNET

<https://artigos.com/artigos/1227-seguranca-em-operacoes-bancarias-via-internet>