A ÉTICA NA UTILIZAÇÃO DO COMPUTADOR

Um computador deve ser utilizado de duas maneiras:

Durante a década de 90, altura em que o computador começou a entrar em casa de cada um, mas muito poucos utilizadores tinham acesso à internet, praticamente a única ameaça informática que havia era uma disquete com um vírus, mas com o advento da internet é a redução dos custos no acesso a ela, bem como com o aumento quer da velocidade, quer com o aumento do tráfego disponível (actualmente é muitas vezes ilimitado) apareceram uma série de novos problemas.

No entanto surgem problemas físicos para os utilizadores: postura, problemas de visão, tempo livre gasto com o computador, etc...

As novas ameaças, através do aumento da sofisticação de vírus com fins maliciosos, que actualmente poderiam ser descritos como os programas mais originais, e mais sofisticados (opinião do autor), em que os objectivos de sua utilização passaram de simples formas de afirmação pessoal dos seus autores, para formas de lucro ilícito baseada no roubo de dados, com o fim de lucrar pelas mais diversas formas como roubo de informação de empresas, acesso a contas bancárias, roubo de identidade, etc. ...

O aumento da oferta no acesso à internet originou também uma nova forma de troca de dados na internet, com a utilização das redes Peer2Peer (mais conhecidas por P2P), originando um aumento acentuado das violações dos direitos de autor, assim como, a difusão de códigos maliciosos na internet (primeiro só existiam vírus agora, aparecem todos os anos, uns bons milhares de novos vírus e novas categorias como rotkits, worms, etc), o aumento da visibilidade de certas práticas como a pedofilia (com a troca de fotos e filmes de menores de maneira transfronteiriça), boatos de terceiros, e outras práticas relacionadas com o que pode ser descrito com a difamação dos indivíduos e até sua dignidade.

Assim para uma utilização mais ética de um computador, um utilizador deveria antes de mais nada utiliza-lo como se a pessoa com quem está a comunicar fosse seu conhecido e estivesse ao seu lado, não virtualmente como está mas fisicamente (não estivesse protegido por uma barreira de anonimato como um simples IP, que pode ser real ou apenas uma camuflagem), assim devo definir num sentido mais técnico uma série de boas práticas para, quer uma utilização mais segura assim como mais humana seja possível.

Manter quer sistemas de protecção actualizada quer regularmente procurar limpar o nosso computador de ameaças que tenham passado pelos buracos do nosso sistema de defesa, protegendo quer a nossa propriedade assim como a de outros.

Evitar utilizar software contrafeito pois podem estar a ser utilizados como meio de entrega de vírus ou falhas de segurança sem contar que é também uma violação dos direitos de autor (respeito e solidariedade).

Proteger quer as nossas palavras-chave de acesso, evitando colocar por exemplo as palavras-chave coladas no ecrã do computador, quer os nossos dados pessoais, recorrendo por exemplo à utilização de *drives* virtuais codificados para guardar dados mais sensíveis.

Ter, sempre que efectuar transacções financeiras, o máximo de cuidado evitando realizar operações que sejam repetitivas, como por exemplo, ter o cuidado de digitar correctamente o código e caso seja pedido novamente abortar, pois apesar de existir um conjunto de ferramentas que permitem codificar os nossos dados (SSL) elas também são vulneráveis á interceptação de por exemplo a entrada no teclado, a visualização de imagens do ecrã (programas que tiram em intervalos regulares imagens), e a gravação de dados do *mouse*, é acima de tudo á falta de experiência, quer á imprudência humana.

Nas compras online se o produto não corresponder ao que foi pedido, denunciar o caso imediatamente, pois na internet essas transacções baseiam-se muito na confiança do que nos está a ser apresentado, a burla é um dos principais receios que evitam um crescimento maior do negócio pela internet.

Nas redes sociais deveríamos evitar colocar dados que possam prejudicar terceiros, menores ou pessoas vulneráveis. Casos nos deparem com tal em vez de ler e ou divulgar deve-se denunciar este tipo de abuso, pois se mantivermos estas redes relativamente controladas as pessoas tem tendência á não abusar delas, mas o inverso também infelizmente acontece.

Não utilizar material como por exemplo pen-drives que sejam desconhecidas ou então que estejam “perdidas” pois como as disquetes dos anos 90, elas também podem ser portadoras de software com objectivos maliciosos (técnica com o objectivo de atacar lojas que tenham especialmente muitos movimentos de financeiros). Com o advento das webcams o anonimato das pessoas tem uma certa tendência a acabar (pois assim pelo menos podemos ver uma imagem da outra pessoa), mas elas criaram outros problemas como o abuso das imagens (desde uma simples foto até conteúdos que podem ser considerados pedófilos) de menores através dos mais variados estratagemas (aliciamento, abuso por inexperiência dos mesmos, até certas formas de chantagem que não necessitam necessariamente de proximidade física para acontecerem). Para evitar isso pode-se instalar software quer de controlo, quer de bloqueio mas talvez o mecanismo mais eficaz seja o de acompanhar as pessoas menos experientes, especialmente se forem menores, é não de os deixarem completamente sozinhos a frente do computador, evitando contudo ser muitos controladores pois isso pode ser contraproducente.

Devemos também fixar um número de horas diário para utilizar o PC mas dando prioridade as tarefas que sejam ou profissionais, ou necessárias como por exemplo entregar o IRS a tempo. Mas devemos também usar para desenvolver á mente a nossa capacidade pesquisar, jogar é construir essencialmente o que poderia ser chamado salto da imaginação proporcionado pela simulação como acontece em jogos como o Civilization.

Não efectuar qualquer transacção financeira na NET através de computador. No meu caso deixei até de consultar o saldo no mesmo depois de ver um conhecido cair na asneira de repetir várias vezes á entrada de códigos numa página falsa da Net, tendo um prejuízo financeiro logo de seguida.

Todas estas medidas visam quer a nossa própria protecção quer a de terceiros que podem ser nossos conhecidos ou até mesmo alguém do outro lado do planeta. Basicamente á regra que devíamos aplicar seria a velha máxima do “não faças aos outros o que não queiras que te façam á ti”, mas como muitas

vezes isso não acontece temos tendência especialmente depois de um susto ou noticia mais alarmista a usar mais a regra do “confia mas vai desconfiando”.