CRÓNICA VISÃO ELECTRÓNICA
Nº 100 / 2010-12-16
http://www.gestaodefraude.eu
Edgar Pimenta

>> A fraude no maravilhoso mundo novo da Internet!

Imagine que vai de férias! Colocaria um cartaz à sua porta de casa a dizer para onde ia? Provavelmente não. Mas sabia que cada vez mais gente o faz?

E o seu número de telemóvel? Gostaria que fosse divulgado num jornal qualquer? Quem sabe um daqueles diários distribuídos gratuitamente... Não? Bem... então ainda não está muito integrado no maravilhoso novo mundo da Web 2.0.

Web 2.0 ??

É uma pergunta válida. O que é a Web 2.0? Havendo muitas formas de a descrever, podemos considerar como a internet onde cada um de nós deixa de ser um mero espectador e passa a intervir, seja através de blogs, redes sociais, etc.. E o exemplo mais fulgurante desta Web 2.0 são precisamente as redes sociais.

Facebook, Twitter, Linkedin, MySpace, Buzz, etc.... Tudo isto são redes sociais. E se acha que é uma moda e que vai passar, desengane-se. As redes sociais estão cá para ficar! Os números são impressionantes. O Facebook, caso fosse um país, seria o terceiro maior país do mundo, ultrapassando os Estados Unidos. O número de amigos/fãs de algumas pessoas ultrapassa largamente a população de muitos países (como por exemplo, da Irlanda).

E as redes sociais deixaram de estar confinadas a cada um de nós, como indivíduos. Cada vez mais empresas, outras instituições e organismos públicos começam a estar presentes nestas redes. Ou seja, a Web 2.0 é a Web do momento.

E sendo a tendência, todos nós lá estamos ou estaremos em breve. E muitos de nós, quando entra nessas redes, "esquece-se" que estamos numa rede mundial e que ao partilharmos informação com os nossos amigos, podemos estar a partilhar essa mesma informação com milhares de outras pessoas, muitas vezes completamente desconhecidas. Ainda recentemente, uma adolescente britânica resolveu convidar alguns amigos para a sua festa de anos. Seja por engano, seja por descuido, o convite foi feito de forma pública e incluía a morada e o telefone da dita adolescente.

CRÓNICA VISÃO ELECTRÓNICA
Nº 100 / 2010-12-16
http://www.gestaodefraude.eu
Edgar Pimenta

21 mil pessoas inscreveram-se para a referida festa. Um caso que, infelizmente, não será único.

Mas e então a fraude? Já percebeu que muita gente não tem consciência dos cuidados que deve ter a sua própria privacidade quando está on-line. Mas o que é que tudo isto tem a ver com a fraude? Simples. As pessoas são uma componente intrínseca à fraude. Seja como defraudadores, seja como vitimas, seja até como colaborantes, deliberada ou inadvertidamente. E a falta de privacidade e divulgação de informação pessoal pode ser usada das mais diversas formas. Vejamos alguns exemplos simples.

Tipicamente, as pessoas usam como passwords algo que seja de fácil memorização e, preferencialmente, com algum significado. São sobejamente conhecidos exemplos tais como o nome e datas de nascimento de familiares próximos (filhos, cônjuge, etc..). Nomes de animais de estimação também não são raros. Enfim… Informação pessoal diversa. E se antes a obtenção destes dados obrigava a algum esforço de pesquisa, entrevistas a pessoas próximas, observação de comportamentos, actualmente essa informação é facilmente obtida nas redes sociais. Muito mais rapidamente e em muito maior quantidade!

Informação que à partida pode ser (ou parecer) inócua, pode ter muito valor para alguns, eventualmente mal intencionados. Peguemos no exemplo inicial: divulgar que foi de férias, que foi dar a volta ao mundo (que era o seu grande sonho) com toda a família não é mais que a demonstração de um estado de espírito. Mas é também a demonstração de que se ausentou da sua residência por um longo período. Uma oportunidade para quem lhe queira assaltar a casa. Paranóia de segurança? Talvez. Mas surgiu recentemente um site que dizia precisamente quais as pessoas que estavam ausentes de sua casa, com base em informação do Facebook e Twitter. E outras existem que permitem obter os números de telefones de pessoas registadas no Facebook. Colocaria essa informação à porta de casa? Pois…. Provavelmente não. Mas se calhar está a fazê-lo…

Mais, essa informação, supostamente do foro privado, pode ser usada por alguém que se faça passar por seu colega ou amigo. Afinal, se alguém chegar perto de si e referir o seu amigo José foi para o outro lado do mundo, com a Maria e os filhos Alberto e Jo-

sefino (tendo deixado o gato Tareco no vizinho), essa pessoa vai logo parecer-lhe familiar. E isto, apesar de ser um estranho que recolheu essa informação na Web 2.0.

Vamos agora supor que eu pretendo realizar uma fraude dentro de uma organização, mas preciso do conluio de alguém. Colaboradores que se considerem injustiçados, mal tratados pela organização e que desejem vingar-se são alvos perfeitos. Facilmente podem aderir a um esquema que, na perspectiva deles, venha colocar alguma justiça na relação com essa organização. E é sabido que empregados descontentes são mais propensos à perpetração de fraudes nas organizações. São por isso mesmo as pessoais ideais para serem abordados por um defraudador quando se procura um cúmplice. E como encontrar alguém nessa situação? Fácil.... Basta procurar nas redes sociais.

Torna-se agora mais fácil iludir alguém a participar no meu esquema sem se aperceber. Para isso nada melhor que me fazer passar por alguém conhecido, o amigo de um amigo. O que preciso? Alguma informação pessoal como nome de amigos comuns, hobbies, nome dos filhos, locais visitados, etc... Um estranho possuidor dessa informação parece logo menos estranho

Mas pode ser ainda mais simples. Posso simplesmente criar um perfil dizendo ser outra pessoa. O perfil, uma vez criado, permite recolher um manancial enorme de informação. Afinal, facilmente se dá informações a um amigo (é a foto dele!!), informações essas que de outra forma, talvez não se desse. Parece fantasioso? Ainda recentemente, uma nova fraude surgiu no Facebook. Um defraudador criou uma conta dizendo ser outra pessoa, informando que a conta original tinha sido comprometida. Adicionou os amigos da conta original e convenceu-os a emprestar-lhe dinheiro, face a dificuldades imprevistas. Quem não emprestaria dinheiro a um amigo em dificuldades?

São as novas formas de engenharia social!

Engenharia social? Mas o que é isso? Nada mais do que conseguir obter informação directamente daqueles que são o elo mais fracos da segurança: as pessoas. É mais fácil e menos exigente em termos técnicos convencer/ludibriar alguém do que entrar em sistemas informáticos. E assim se ultrapassam os controlos instituídos levando alguém a confiar em nós, realizando acções que

CRÓNICA VISÃO ELECTRÓNICA
Nº 100 / 2010-12-16
http://www.gestaodefraude.eu
Edgar Pimenta

podem pôr em causa a segurança dos sistemas e da informação que estes albergam. E para que alguém confie em nós, nada como parecermos alguém familiar, alguém com quem partilhamos interesses semelhantes ou simplesmente, alguém que compreende alguma situação complicada pela qual o nosso "alvo" está a passar. E como obter informações que nos permitam criar a ilusão dessa proximidade? Actualmente, da maneira mais cómoda e fácil possível: sentados na secretária, mergulhando do maior manancial de informações pessoais - a Web 2.0. E ainda estamos no início.... Por isso, use as redes sociais com prudência da informação que aí partilha.

Estamos a sugerir-lhe a não utilização da Web 2? Não, estamos a aconselhá-lo que seja muito prudente.