Are You Safe On-line?

What you don't know will send your bank details to Russia!

Introduction

When Apollo 11 made its historic landing on the moon, the total computing power in the landing craft was far less than you have in your pocket or purse right at this moment. The massive 64k of memory that they had on board meant that they could get the job done, but the various applications they used had to be "swapped" in and out of this memory space to be able to function. It was hardly "user friendly"!

Meanwhile, back in Houston, the team led by the irascible Gene Krantz had rooms full of mainframe computers cranking out lots of heat and the data vital for the mission to succeed. This was in 1969. By 1985 the commodore 64 was delivering the same computing power right there in your living room for less than 0.3% of the price. Right now the phone in your pocket has more computing power than large banks or insurance companies had 20 years ago. Such is the massive rate of change in the world of IT.

The problem

What has happened in this dramatic period of time is that the computer has become ubiquitous. Back in 1985 the primitive data links between computers consisted of modems and bulletin boards and cassette and (DAT) Digital Audio Tapes. The internet was merely a twinkle in Al Gore's eye!

Today, the computer is embedded in everything and connected to everything else. It has become the networked computer and the advent of cellular and wireless networks means that we are always connected to all our devices all the time whether we like it or not.

The consumerization of the computer is the problem. When people are marketed to, they get the glamour and the glitz, not the dire warnings of what may go wrong. This imbalance between the Risk and Risk

About netlogx:

Founded in 1998, netlogx is an Information Risk Management company that specializes in working with our customers and consultants to solve complex business problems.

We provide Project, Security and Information Management services and products that enable our customers to get "Better, Faster, Cheaper" and thrive by effective and efficient Risk Management.

Perception is at times staggering. What people will do, say on line is only dwarfed by the lack of protection that they will assign to their devices and data. However, all of this pales into insignificance with the very real potential disasters that exist in an internet connected world.

The Risk

There are billions of people using the Internet every day for work and play, often at the same time! The growth is mind-blowing. In just 5 years the number has gone from 1.3 Billion to 2.26 Billion. As you would expect the transactions for searches, emails, texts and social media have had explosive growth, but what underlies the data is that people are now doing "real" things on the internet. They shop; they do their banking and the conduct commerce online to the point where many institutions will not interact with customers without an online persona.

But here's the big risk; all of this requires the collection and management of personal and financial information, the stock and trade of the emerging cyber criminals. In order to ply their trade, criminals of all types are deploying malware at a staggering rate. In 2006 there were 57 new attack vectors being unleashed each day. At the time of writing this number is now 6,300 **per hour**!

Identity theft, bogus banking transactions and credit card theft are all now all too easy to perpetrate.

The Risk Perception

So why are people not scared enough to change the way that thing happen, either as a consumer or as a provider? The main reason is what is termed Risk Perception. What that means is that after millions of years of evolution we still make Risk decisions at an emotional level. In simple terms we don't employ our head and reasoning often enough. We react to the "Rainbows and Unicorns" that the marketing presents us with rather than the cold hard and unpalatable facts. The providers of services through online mechanisms work hard to make the friendly side of the equation outweigh the security side and they are also only driven to take action after there have been issues and even then only where there is threat of legal action.

Risk Reality

As a compromise, I will spend the remainder of this presentation explaining in cold hard unpalatable facts what is actually happening, but I will present it in a very friendly manner!

Let's concentrate on the following topics:

- Social Media – The Do's and Don'ts!
- Phone Security – What you don't know will send your bank details to Russia
- Internet and email Security – Your mission critical application

Social Media

Social Media is the most fertile ground for cyber criminals. People will do very stupid things in social media settings that they would shy away from in the "real" world. They will publish personal information including bank account details, passwords and other crucial data, seemingly without a care in the world. The will also

respond to notes and emails that are specially designed to garner this information and build a profile of individuals. The tools themselves encourage this kind of behavior and are basically only as secure as the weakest link in a person's social network. By that I mean that the data you protect is unprotected once you share it with someone who is not as cautious or conscientious. Criminals use surveys, which appear to have come from a friend or contact, to garner information, which on the face of it might appear to be trivial in the context of a survey but may be used to attack bank accounts. A great example of this is the security questions your bank asks you. What is your mother's maiden name? What was your first car?

The other attack vectors on social media are things like; urgent messages sent to you telling you that someone you know is stranded and they need you to wire money, messages telling you that there has been a security breach and that you need to change your password by following a link that they conveniently provide.

With the most innocent of response you can compromise your entire identity.

Social Media is also a well-publicized battle ground were cyber bullies can make people's life a misery. Some of the mechanisms for doing this are again provided by stolen information. Facebook even has people advertising other stolen or compromised data. Ironically they want payment via PayPal!

Our advice on Facebook is simple. Don't use it and don't let anyone you care about use it either.

Phone Security

Facebook make no bones about the fact that they gather everything about you and sell the information. Their application on the phone is designed to gather information from other applications on your phone. So, if you have anything of value on your phone, think twice or three times about having Facebook in the mix, especially if it involves banking or shopping and the collection of personal information.

Facebook is not alone in wanting preposterous rights to the information on your phone. Many ad supported applications track where you are so that they can serve up relevant content. There are however many emerging application threats where there are simply malware in the guise of a game or social media tool.

Your phone is a computer and can be infected with virus and malware in the same way as your laptop. Make sure that use an Anti-Virus product. Make sure that you don't just click through when you are loading an app. Look at what permissions are being asked for and if they don't seem right don't load it. Remove anything that you are not using. Regularly clean up the phone and always make sure that regular updates, especially as they relate to security, are applied.

Phones should be password protected and treated as you would treat your wallet. Don't let it out of your sight as they are a frequent target of theft.

Internet and email security

The internet is not a place for the faint hearted. It is becoming, literally, a battle ground as Chinese Army Hackers attack US infrastructure and steal anything they can as well as destabilizing critical infrastructure such as power and water. People are lost without their email and in businesses and families alike it is the mission

critical application. As such it's vital to get serious about protecting yourself whilst using it. Everything that we covered above about social media and phones applies to email.

If you use the internet and email then you must know the risks and you must protect yourself, your family and your business by being:

- Educated - Make yourself aware of these risks and keeping current with their development
- Secure - Use Strong Passwords or two and three factor authentication where possible – yes it takes longer but trying to get your identity back will take far more time
- Securer – Encrypt your hard drives and files
- Smart - Don't download files and videos from sources you cannot be sure of
- Smarter - Don't follow URL links from sources you cannot be sure of
- Wise - Insist on Antivirus and other security tools – yes even you apple users!
- Ready - If it doesn't seem right don't do it

netlogx services

netlogx will be delighted to offer security awareness programs to any organization, big or small, that would like to take advantage of it. We can deliver these programs locally as well as over the internet. If you know a business, a school or other institution that would like to get stronger one user at a time please pass on our details.

We also offer comprehensive testing and assessment services that can help you to "harden" your infrastructure and processes to meet the challenges we now all face online.