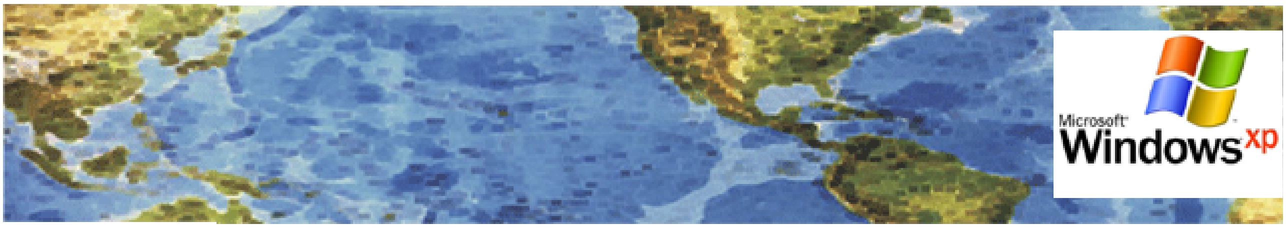
HALL ASSOCIATES



Risk-Based Decision Making Commentary

25 August 2013 Newsletter

The End Is In Sight – For Windows XP Support that is.

Microsoft will cease support for Windows XP on April 8, 2014, and disasters of biblical proportions could follow! Unprotected by continued security patches, Windows XP could become a festering wasteland where banking Trojans rob people blind, shifty criminals hijack little old ladies' computers on a whim, and innocent PCs get drafted into botnets to work at exploitative data mines all day long.

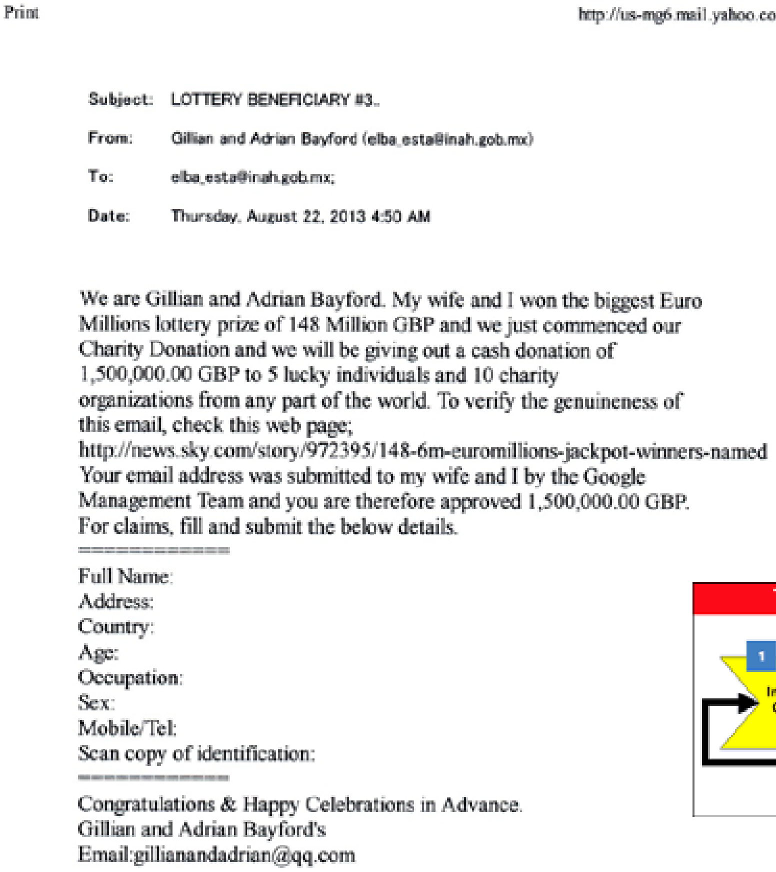
OK, the above scenario might be a little extreme, but Windows XP users (of whom there are still a huge number) have known since April 2013 that XP's days were numbered, and many of them have yet to switch over to Windows 7 or 8. Come April 2014, this will make Windows XP into a haven for malicious hackers, as users will have little recourse against new forms of malware.

The threat of malware is pressing. As long as Windows XP has a sizable user base, it will remain a tempting target for purveyors of harmful software. After April 2014, Windows XP will not receive any more security updates. Savvy users can still avoid and treat malware, but others will find their systems infected and have little to no recourse. There are supposed to be people developing XP exploits and saving them up and waiting till after the sundown date. In any case, there are people who figure out how to exploit various operating systems and sell them to someone else to actually develop the malware. This is a serious and growing marketplace. A few new malware types might not be a major problem, but a gradual buildup almost certainly will. Every time a new problem in XP is found, those things will build on one another, month after month, and the risk will increase almost exponentially over the next few years.

Note that most Windows 7 and 8 bugs are based on the core Windows software, **which has not changed since Windows 95**. This means that when Microsoft releases patch notes for 7 and 8, it will give exploiters a number of easy new ways to compromise XP. Three or four new bugs each month may seem harmless, but the problems will be additive; within a few months, an XP system could be vulnerable to 15 or 20 crippling flaws. And the only recourse you have, if you are not a security developer able to correct your system yourself, is to change to Windows 7 or 8.

http://www.tomsguide.com/us/windows-xp-malware-deluge,review-1872.html?cmpid=532509

New Version of Email Scam (At least to me)



Print http://us-mg6.mail.yahoo.com/neo/launch?.rand=a1cple21c037h#mail

Subject: LOTTERY BENEFICIARY #3.

From: Gillian and Adrian Bayford (elba_esta@inah.gob.mx)

To: elba_esta@inah.gob.mx;

Date: Thursday, August 22, 2013 4:50 AM

We are Gillian and Adrian Bayford. My wife and I won the biggest Euro Millions lottery prize of 148 Million GBP and we just commenced our Charity Donation and we will be giving out a cash donation of 1,500,000.00 GBP to 5 lucky individuals and 10 charity organizations from any part of the world. To verify the genuineness of this email, check this web page; http://news.sky.com/story/972395/148-6m-euromillions-jackpot-winners-named Your email address was submitted to my wife and I by the Google Management Team and you are therefore approved 1,500,000.00 GBP. For claims, fill and submit the below details.

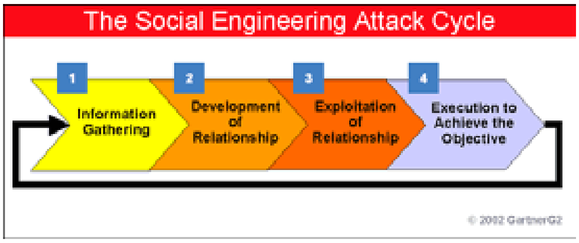
============

Full Name:
Address:
Country:
Age:
Occupation:
Sex:
Mobile/Tel:
Scan copy of identification:

============

Congratulations & Happy Celebrations in Advance.
Gillian and Adrian Bayford's
Email:gillianandadrian@qq.com

Hacker's polite approach works like a charm



The Social Engineering Attack Cycle
1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective
© 2002 GartnerG2

Social engineering, in this case the e-mail, is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access. Fraudsters are perfecting their abilities to target and manipulate people. Well-crafted social engineering schemes take advantage of common user behavior. While this e-mail may look dumb and you think "No one is their right mind would fall for this" it is really a great example of social engineering. Only those ignorant enough, greedy enough or desperate enough will respond, thereby minimizing the scammers task of getting people to work on. Don't click on unknown links or **provide personally identifiable information** to someone you don't positively know. I would not recommend going to the referenced web site just to see what this is. In some cases that's all you need to do to download malware. The best way to avoid being scammed is by knowing what to look for and to NOT give out any personal information to anyone unless you absolutely know who you are giving your information to.