NEWS RELEASE

Survey finds 1 in 4 kids have tried hacking!

School computers a great avenue to hack friends
Facebook and email accounts – all child's play!

London, 18th March 2010: Despite 78% agreeing that it is wrong, 1 in 4 of UK's children have tried their hand at hacking into others' Facebook accounts mostly by surreptitiously using the victims passwords– that is the stark finding of a survey released today. And it's not just the boys – 47% admitting guilt are girls. The study of 1,000 youngsters from London and 150 from Cumbria found that although 27% were doing so from the relatively safe confines of their bedrooms, these juvenile offenders are utilising computers in Internet Cafés (22%), the ICT suite at school (21%), and a friend's machine (19%). The most common reason was for fun (46%) however 21% aimed to cause disruption and a resourceful 20% thought they could generate an income from the activity. A small minority (5%) were switching to the dark side as a career move!

It's not all one-sided though, as the kids revealed they'd also fallen victim with over a third having had either their Facebook or email account hacked.

Conducted by IT security experts Tufin Technologies in conjunction with Cumbria Constabulary, the survey surprisingly revealed that the Cumbrian children with hacking habits were much younger than their city counterparts, with 78% having done so before their 13th birthday – in London 44% were under 16 with only 16% of these yet to enter their teens.

When the survey dug a little deeper it unearthed that of the children who had hacked over a quarter had targeted Facebook accounts, 18% went for a friends email, 7% for online shopping sites, a cheeky 6% besieged their parents email, and 5% breached the school website. A bold 3% had honed their skills enough to aim much higher with corporate websites under their belts.

It's not all doom and gloom - there is some comfort to be drawn from the 27% of our apprentice criminals that were caught. 82% of the sample confessed hacking wasn't actually that easy in practice and a commendable 70% labelled the practice as 'uncool'!

Cumbria Constabulary's Deputy Chief Constable Stuart Hyde ACPO lead on E-Crime Prevention and President of the Society for the Policing of Cyberspace (POLCYB), an organisation which sees law enforcement and industry working together to increase people's personal and professional knowledge of cyber crime issues said: "What this survey starkly highlights is that hacking into personal online accounts whether email or Facebook can be child's play if users do not protect their own passwords. It illustrates the importance of keeping your passwords strong, secure and changing them regularly to help protect your accounts from unscrupulous people of all ages. We live in a world where social networking, email and the internet are embedded into our every day lives from a far younger age so early education is essential to ensure young people know the devastating consequences this activity can have."

“Only 53% of the children surveyed felt that hacking (i.e. using someone else’s account) was illegal which shows there is a real need to educate youngsters to the dangers both so they are deterred from trying it and also so they know how to protect their own accounts. Hacking is illegal and we need to ensure everyone understands that,” Hyde concluded.

Picking up from this point, Reuven Harrison, CTO and Co-Founder of Tufin Technologies said, “One of the most worrying statistics from this survey is the staggering numbers of kids that are successful and the ages involved. Hacking has changed a lot in the past few years from the curiosity or fun factor to now making serious money or causing havoc in the corporate environment. Our job as IT security professionals is to stop hackers in their tracks and that means educating the kids as the Police have said at a very young age.”

One lesson from this study is that if our children are able to hack these types of sites, then it must be child’s play for those with criminal intent. However, there are some things that can be done to protect our online activity:

1. Install security software: anti-virus, anti-spyware and a firewall
2. Never disclose passwords or respond to emails that ask us for this information
3. Vary your user name and passwords between sites. That way if one account is compromised it can limit the damage of others being breached
4. Untick ‘remember me’ boxes for user name and passwords, especially for email accounts, online banking, social media websites etc. if your computer is used by other members of the household – and therefore possibly their friends
5. Be careful what you talk about in chat rooms, you never know who you’re talking to or who’s listening in. Someone with an ulterior motive could be gathering information spanning many months that individually tells you nothing but pieced together provides a complete picture
6. Periodically change your username and password, immediately if you suspect someone may know it.
7. Protect yourself against eavesdroppers and freeloaders by using encryption on your wireless network
8. Use a password manager such as Password Safe by Bruce Schneier (http://passwordsafe.sourceforge.net/)

To find out more about how to protect yourself online log on to: www.cumbria.police.uk/advice-and-information/crime-prevention/on-the-web

About Tufin Technologies, Inc.
Tufin™ is the leading provider of Security Lifecycle Management solutions that enable companies to cost-effectively manage their network security policy, comply with regulatory standards, and minimize IT risk. With a combination of accuracy and simplicity, Tufin empowers security officers to perform reliable audits and demonstrate compliance with corporate and government standards. Founded in 2005 by leading firewall and business systems experts, Tufin serves more than 500 customers in industries from telecom and financial services to energy, transportation and pharmaceuticals. For more information visitwww.tufin.com, or follow Tufin on:
Twitter at http://twitter.com/TufinTech,
LinkedIn at http://www.linkedin.com/groupRegistration?gid=1968264,
FaceBook at http://www.facebook.com/group.php?gid=84473097725,
The Tufin Blog at http://tufintech.wordpress.com/,

The Tufin Channel on YouTube at http://www.youtube.com/user/Tufintech

If you would like to organise an interview with DCC Stuart Hyde please contact Joana Dowling at Cumbria Constabulary Press Office on 01768 217009 or Michael Baker at ACPO Press Office on 0207 084 8408.

Stuart Hyde is Deputy Chief Constable of Cumbria Constabulary and ACPO lead on E-Crime Prevention and President of the Society for the Policing of Cyberspace (POLCYB). POLCYB is an organisation which sees law enforcement and industry working together to increase people's personal and professional knowledge of cyber crime issues.