Children & Cyber Security

Helping Our Children Stay Safe in a Digital World

Cyber security in the context of business is a very real topic and occupies much media space.

Perhaps not quite so talked about are the cyber issues surrounding children and the ensuing security risks surrounding them.

Personal Information

Most of us educate our children about the dangers of sharing personal information online, either of themselves, or their family members. In this day and age, it would be fair to assume that children would know better than to post credit card details, identification numbers, addresses, or passwords online.

What is less evident perhaps, is the danger in sharing other private information - information that could also have significant implications.

For ultra-high net worth (UHNW) individuals, one of the biggest fears is the personal safety of their family. Evidence suggests that people in positions of wealth, and their families, are being targeted more and more. In the context of the Family Office, this can have profound effects. Determined cyber criminals will take advantage of any information available to them in their attempts for personal gain.

Details of pending holidays, personal struggles, or locations, for example, are the sort of details that cyber bullies and predators look for. Sometimes, this information can be all that a harmful individual needs to threaten, intimidate, extort or even abduct children.

Professional help is available in terms of analysing and mitigating the risk, entailing full investigations on the individuals' online footprints, and requisite cyber education around online profile management. Reputation management consultants are also highly valuable, both from a precautionary focus (often through experience of acting for UHNW individuals and celebrities) and post threat (possibly enlisting the resources of public relations consultants, media and legal services).

Phishing/Smishing

Using emails to trick children into clicking on malicious links is common and, because many phishing attempts are couched in child-friendly terms (“Hey, is this you?” “Look what I found!”), such scams are often successful. Malicious links enable cybercriminals to gather information on children in the same way that corporates are targeted.

As children are more likely to be on their phones than emailing, smishing is also popular - using messaging apps or text messages to achieve the same result.

Timely family discussions around avoiding clicking emails or messages from unknown persons, are critical to avoid system infiltration.

Internet of Things

When considering children and cyber security, the risks are much wider than those just related to the use mobile devices. The Internet of Things has revolutionised the way we operate on a day to day basis. The use of internet-connected devices, while hugely convenient (think Alexa, “smart” speakers and watches, or mobile gaming) brings a level of risk to our children that can too easily be overlooked. The transmission of data to and from the internet brings with it issues around the security, exploitation, use and commercialisation of that information.

Recently we learnt about a vulnerability affecting Real Time Streaming Protocol.

Indications were that up to 110,000 open camera streams were uncovered which enabled hackers to view, among other things, video footage streamed from child day-care centres or baby monitors.

Terrifyingly, this vulnerability has the potential to allow harmful individuals access to children’s personal spaces and private images.

Suggested actions to ensure only authorised people have access to the images include:

1. Ensuring a RTSP camera requires parties to enter a password each time they connect to a video stream;
2. Ensuring that any baby monitoring device is legitimate and not a repackaged wifi webcam which are able to be misconfigured more easily, thereby allowing unauthorised access.

“Smart” interconnected toys also pose risks. The ‘Internet of Toys’ refers to toys based on voice or image recognition, app-enable robots and other toys connected to the internet. Complaints have been raised over the compromise of children’s rights to privacy and safety; there are increasing calls for software designers to build in safeguards to their products.

Vigilance and awareness are key. Guardians and parents are encouraged to be watchful and informed and, where appropriate, educate children of the increased risk.

For further information please contact Vanessa Cathie or Rachel Gilliam.

Vanessa Cathie – Vice President, Global Cyber & Technology

Lockton Companies LLP

The St Botolph Building | 138 Houndsditch | London | EC3A 7AG

T: +44 (0)20 7933 2478 | **M:** +44 (0)7 7804 87830

E: vanessa.cathie@uk.lockton.com

Rachel Gilliam – Partner, Head of Private Clients

Lockton Companies LLP

The St Botolph Building | 138 Houndsditch | London | EC3A 7AG

T: +44 (0)20 7933 2605 | **M:** +44 (0)7958 784593

E: rachel.gilliam@uk.lockton.com