

## Trainer Bio Profile – ANDY PRAKASH



<https://www.linkedin.com/in/andy-prakash/>

Andy Prakash is a recognized cybersecurity expert, an accomplished entrepreneur, and a thought leader in data protection, with a career spanning over two decades in the technology and information security sectors. He co-founded AntiHACK.me, the pioneering bug bounty platform in Singapore, which teams up with an elite community of ethical hackers to detect and report vulnerabilities in businesses' digital infrastructure.

In his role as the Chief Information Officer, Andy has been instrumental in driving awareness about the criticality of cybersecurity. His influence extends beyond traditional business circles, demonstrated by his invitational speeches and free masterclasses delivered to diverse audiences, including ACE startups, co-working spaces, Chamber of Commerce, and Interpol World. His live hacking demonstrations at Echelon, NTU Alumni Club, and other platforms have shed light on the imminent dangers lurking in the cyber world.

Identifying an industry-wide gap in data protection, Andy took the initiative to establish Privacy Ninja. As a comprehensive solution provider, Privacy Ninja offers PDPA Consultancy, training, audit, and outsourced DPO services. Andy personally serves as the designated Data Protection Officer (DPO) for a broad array of companies in Singapore, managing their day-to-day data protection issues.

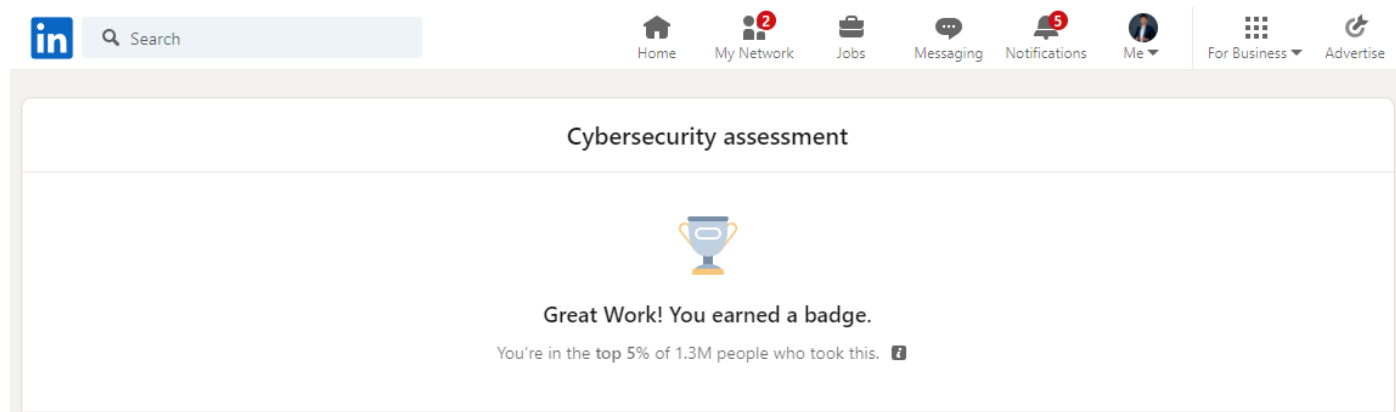
With a client portfolio of over 300 organizations including Marina Bay Holdings Group, Adam Khoo Learning Technologies, Curtin University, Marche Restaurant, Astons

Group, Civil Service Club, OhMyHome, J&T Express, and others, Andy's data protection expertise is widely recognized and sought after.

As a thought leader, Andy has been regularly featured in multiple high-profile media outlets such as Business Insider, Yahoo News, Channel News Asia, The Straits Times, and Channel 8, Lian He Zao Bao, Channel 5 among others. His insights and opinions on data privacy, cybersecurity, scams, OSINT and related topics have informed and guided businesses and individuals alike.

Andy's passion for teaching, training and creating awareness was not newfound, and was shaped from as early as working as a tuition teacher in his early tertiary education days, an SAF Officer during his National Service and eventually into corporate training.

Equipped with a robust track record in cybersecurity and data protection, Andy extended his expertise to OSINT (Open Source Intelligence) training. His vast experience and understanding of the cybersecurity landscape will prove invaluable in shaping the future OSINT professionals, enabling them to navigate the complexities of open-source intelligence in a cyber-centric world.



### **LinkedIn 2023 Professional Cybersecurity Assessment**

#### **Media Feature Links:**

<https://markets.businessinsider.com/news/stocks/privacy-ninja-s-dpo-as-a-service-bolsters-data-protection-cybersecurity-of-over-200-organizations-in-singapore-1030676749>

<https://www.digiconasia.net/news/dpo-as-a-service-launches-in-singapore>

<https://marketinginasia.com/2020/10/09/privacy-ninjas-dpo-as-a-service-aims-to-raise-the-level-of-digital-security-for-businesses-in-singapore/>

<https://e27.co/this-whitehat-slash-co-founder-taught-me-that-when-it-comes-to-data-privacy-ignorance-is-never-bliss-20200527/>

<https://www.channelnewsasia.com/news/technology/singapore-start-up-antihackme-catches-computer-bugs-10686008>

<https://www.8world.com/news/singapore/article/darknet-934386>

<https://www.youtube.com/watch?v=MaHBA7iKU0M>

<https://www.beritaharian.sg/ekoniaga/rekrut-penggodam-bantu-firma-perbaiki-keselamatan-siber>

<https://www.8world.com/news/singapore/article/20180918-sg-international-cyber-week-322161>

<https://www.youtube.com/watch?app=desktop&v=zW4vKnO4sMQ>

<https://news.yahoo.com/privacy-ninjas-dpo-bolsters-data-131500388.html>

<https://www.straitstimes.com/singapore/more-children-cheated-in-game-scams-counsellors-urge-peer-support-and-parental-supervision>

<https://www.zaobao.com.sg/news/singapore/story20220207-1240044>

<https://www.straitstimes.com/singapore/more-children-cheated-in-game-scams-counsellors-urge-peer-support-and-parental-supervision>

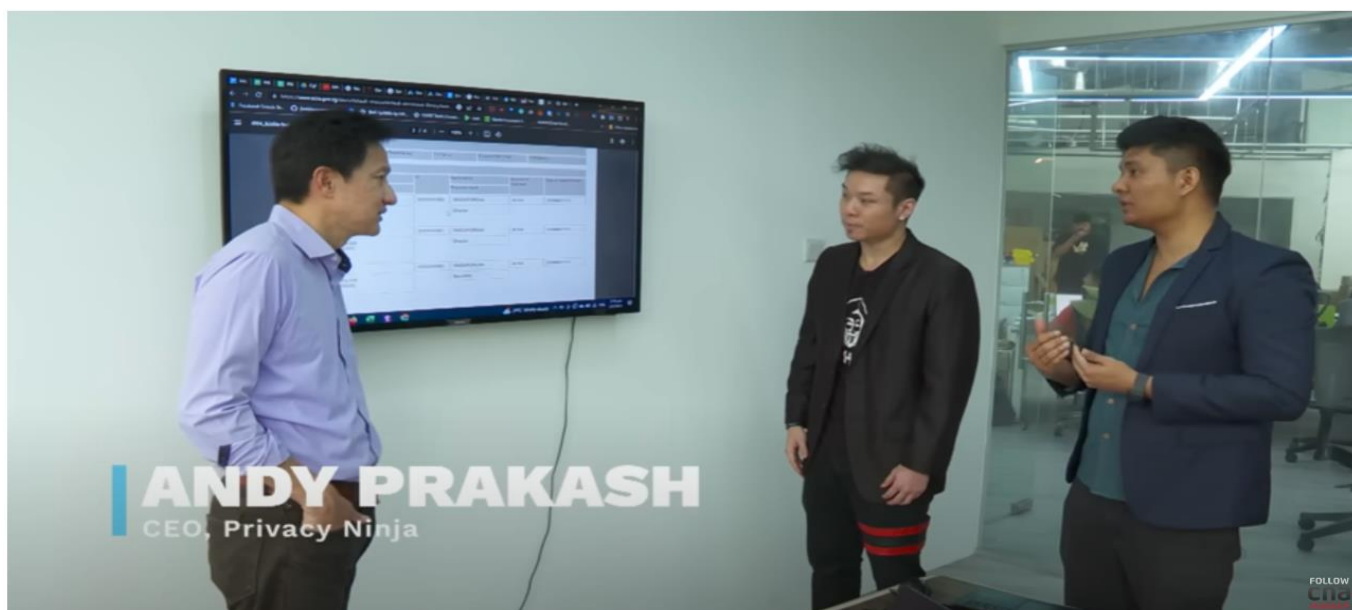
<https://www.straitstimes.com/singapore/how-a-stranger-can-cancel-your-next-holiday-with-just-a-photo-of-your-boarding-pass>

<https://www.straitstimes.com/singapore/courts-crime/at-least-562-million-lost-to-business-e-mail-compromise-scams-between-jan-and-march-2022-police>

<https://www.youtube.com/watch?v=Px7DR3-V4mc&list=PLkMf14VQEvTai524iU74UlzpWvb1RRAvI>

<https://www.youtube.com/watch?v=jEtj4jEURKU&t=64s>

## Sharing of OSINT techniques for Channel NewsAsia – Talking Point April 2023



Link: <https://www.youtube.com/watch?v=Px7DR3-V4mc&list=PLkMf14VQEvTai524iU74UlzpWvb1RRAvI>

## Corporate Training Experience



**Data Protection (PDPA)**



**Cyber Hygiene**



**Cybersecurity**

## Speaking / Interview Features



**CNA Money Mind**



**e27 Live Hacking**



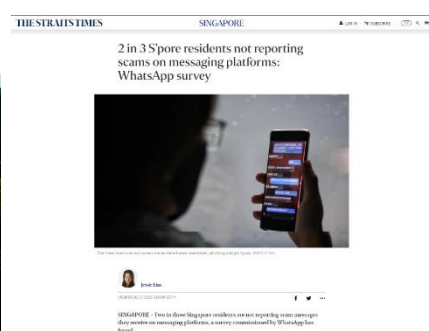
**Talking Point**



**Chamber of Commerce**



**Interpol World**



**Straits Times (Scams)**



**Channel 8 (GovWare)**



**Channel 8 (Dark Web)**



**Channel 8 (Home Security)**

本报专访两白帽黑客 钓鱼骗案本地化或有内行人策划

无论是导致人心惶惶的银行钓鱼短信骗案，还是近日扫QR码领优惠券、国内税务局官网领钱等，犯罪团伙在设计骗局时，专门针对本地人，以获利作为最终目标。

刘芸如 报道 liuyunru@sph.com.sg

钓鱼骗案环环相扣，经过精心布局，背后是具有有一定商业模式...

针对近期的几种钓鱼骗案，《联合早报》专访两名白帽黑客——隐私忍者(Privacy Ninja)联合创始人方绍宇和威联集团(Wizllynx group)亚太总裁廖金福...

白帽黑客，是指利用黑客技术和协助企业或机构测试网络安全和系统性能的善意黑客。

无论是导致人心惶惶的银行钓鱼短信骗案，还是近日扫QR码领优惠券、国内税务局官网领钱等，犯罪团伙设计出钓鱼的情

节，诱导受害者点击钓鱼网站，通过骗取对方的个人资料、银行信息等得手。

犯罪团伙在设计骗局时，专门针对本地人，以获利作为最终目标。以银行钓鱼短信诈骗为例，当犯罪团伙设计脚本时，他们须邀请熟悉金融行业的知情人士...

廖金福指出，这并不排除此类骗案的参与者有离职的前银行职员，或是熟知行业模式的金融从业者。方绍宇说，因为脚本得“在地化”，因此犯罪团伙中必有本地成员，甚至部分是本地团队。

经过与知情人士、本地成员几轮沟通后，犯罪团伙已经能事无巨细地掌握业内流程，从中发现短信中的链接可以作为突破口，因此才设计了钓鱼短信诈



威联集团亚太总裁廖金福指出，犯罪团伙早已牢牢掌握了受害者的心理盲点，让他们轻易陷入骗局。(白帽琳摄)



隐私忍者联合创始人方绍宇。(白帽琳摄)

骗。行骗过程中，犯罪团伙成员也分工明确。如“行动组”负责计划与执行各部门活动，包括获取受害者登录信息和密码等；“技术组”负责网页寄存(web hosting)、购买域名、通过软件群发短信电邮等；“营销组”须搜集线索建立受害者档案，大量购买手机号码等数据；“金融组”负责准备第三方或是代收账

户，通常是向负债累累的个人提供网贷，让对方借出银行账户或申请新账户，或是从即将回国的外国人手中购买账户资料；“网络安全组”则会使用伪造的身份信息来注册网络账户，利用VPN在行骗时隐藏IP地址。

经过一番精密的部署后，诈骗团伙坐等受害者落入骗局，获取相关信息，他们利用获取到的个人资料信息，可以在另一部手

机上进行操作。

在银行钓鱼短信骗案中，不法分子就接管了受害人的银行账户，绑定新的联络号码，提高转账额度。诈骗团伙还会陆续在账户内添加多个收款人，将钱款逐一转出，也会时刻盯紧转账上限，避免触发银行的通知短信。或者看准时间在凌晨时分进行转账，这样即便有通知短信发送，受害者可能因在睡梦中而错失

举报的最佳时机，睡醒发现时已晚。当钱财到手后，不法分子可能通过第三方账户从自动取款机取走现金，当然已经进行一定的伪装，避免镜头捕捉到对方的脸。不法分子也可能直接通过快速海外汇款服务转移资金、购买加密货币，或是直接用于购买一些昂贵物品。

复制网站只需一分钟

钓鱼网站背后的组织可能严密，但技术本身并不复杂，甚至只需一分钟就能复制出假网站。

犯罪团伙十分善用公开的网络资源，轻而易举便能制作出钓鱼网站。比如，黑客只需打开任何网站的页面，后台复制网站编码，一分钟内就克隆出一个以假乱真的钓鱼网站页面。即使网站页面中一些图片、影像资料需做调整，对于黑客也不是难事，最多花上半个小时就能修改好。

黑客只须具备最基础的编码知识，便可以在钓鱼网站上创建一个后端窗口，或是转发程序，坐等受害人上当，轻松获取他们的个人资料。

制作好网站页面后，黑客便会上网购买与官网网站相似的域名，这些网址可能与真正官网只有一个字符之差。以方绍宇提供的其中一个购买网站为例，记者只须输入自己想要购买的网站网址，网站立刻显示出该网址是否可以购买以及价格，下方更会出现一系列类似的网站地址供顾客一并购买，而这些网址的价格每年只需7美元(约9.5新元)到10多美元不等。

值得注意的是，这些黑客在



克隆一个钓鱼网站页面只需一分钟，加上最多半个小时修改就能以假乱真。黑客在钓鱼网站上创建一个后端窗口，或是转发程序，坐等受害人上当，轻松获取他们的个人资料。

注册或购买网站时，他们都会掩饰真实身份，通常姓名、注册信息都是伪造的。用于付款的借记卡也是一次性的，在某些情况下，他们甚至会使用加密货币来付款，来防止被追查。

廖金福说，犯罪分子可能一次过购买多个网址，同时拥有多个可用的网站网址，也提前做好

备份，一旦其中一个钓鱼网站被当局取缔后，不法分子立刻可以激活其他钓鱼网站继续行骗。他表示，因为这些网站的供应商可能来自不同国家和地区，申请取缔网站的时间和规定也会不同。

方绍宇说，除更换网址外，若钓鱼网站被取缔，黑客们完全可以将同一个网址更改至另外一

个托管供应商，或只须花几分钟时间，钓鱼网站就可恢复运作。

他说，黑客们为了让网站看起来更真实，甚至还会申请SSL(Secure Sockets Layer)凭证，就是网址前会出现密锁图标，但实际上任何人都可以在网上免费申请SSL凭证，不能以此来判断是否是钓鱼网站的依据。

专家：应将多方查证应用到生活

为防止受骗，公众接到网络或社交平台的指示或邀约时，应先多方查证才回应。

《联合早报》记者在为本篇报道采访时，通过业内人士拿到了网安专家廖金福的联络，并通过WhatsApp联系他，在表明身份后也向廖金福提出约访邀请。

对方在收到邀约后，首先确认了记者是通过业内好友获取他号码的方式，过后进一步询问记者的姓名和就职部门。记者同时也将自己的名片照片发送过去。不久后，廖金福发来了记者的LinkedIn截图，并向记者确认，双方添加好友。在后续的电访中，廖金福也要求通过视讯进一步验证记者的身份，并在首次访问结束后，约时间面谈。上述便是一个“多重认证”(multi-factors authentication)的生活实例。

廖金福指出，犯罪团伙在施展骗术时早已牢牢掌握了受害者的心理盲点，让他们轻易陷入骗局。像此前的银行诈骗

短信案件，诈骗团伙精准掌握客户平时的行为习惯，即不少客户会关注银行平台发送来的通知短信，并且潜意识里认为这些短信内容是可靠的，因此不加防范地点开短信中提供的链接。“为了避免受骗，公众应该具有多重认证的意识，将它应用到实际生活中。”

同时，本地的生活、工作节奏快，公众有“怕输心态”，加上人们都具备掌握信息科技的一定能力，当收到来自政府或当局的电邮、短信时，自然会想要立刻采取行动了解情况。诈骗团伙也明白公众的这种心态，布下了圈套。

另外，疫情当下，政府推出的一系列经济援助措施，加上准备调整消费税的政策，一些公众会抱着等待福利、优惠等占便宜心态。

另一白帽黑客方绍宇说：“如果一件事情好到你难以置信，那么就相信自己的直觉别想了，那可能就是假的，千万谨慎处理。”

新加坡

## 互联网之外：暗网 提供买凶杀人等非法服务

文：李贇谊 发布：29/09/2019 23:12 更新：29/09/2019 23:12 ☆ 收藏



网络世界无边无际。除了我们很熟悉的互联网之外，其实还有所谓的“深网”，当中的内容是用标准搜索引擎无法搜索到的。而“深网”之中，还有一个部分叫做“暗网”，只有利用特殊软件或是被授权才能进入。在这里，人们可以购买枪械、被盗取的个人资料、假护照等等，甚至买凶杀人。

我国去年发生一起买凶杀人事件。一名47岁已婚男子，因眼红前情人另结新欢，通过暗网请了一名杀手，要求制造假车祸杀害前女友的新欢。

男子支付了价值8000新元的比特币，但在行动的五天前，被警方逮捕。据报道“杀手”其实是个诈骗网站，而我国是在接到一名美国记者的通报后展开调查才被案的。

要潜入暗网需在互联网上仔细搜索各种蛛丝马迹，通过特定网址才能找到通道。为了掩人耳目，同时甩开执法人员的跟踪，这些网址往往是毫无意义的一组乱码，而且会不时更新。

AntiHACK.me联合创始人白帽黑客方绍宇表示：“我们不鼓励大家进入暗网，因为在找东西的时候，可能你不知不觉会下载到一些恶意软件，导致你的电脑中毒。还有你在暗网买了东西之后，你有可能被对方勒索，如果他们能查到你用哪一架电脑买的。如果你没有好好保护自己的系统或IP地址等等，会比较容易被勒索。”

据了解大约七成在暗网交易市场上购买产品或服务的人，都会选择使用虚拟货币，例如比特币来进行交易。因为这样比较能够确保他们的身份保持匿名。

浏览暗网并不犯法，不过一旦涉及非法活动，例如下载色情片、购买被盗资料或黑客工具等等就违法。我国目前没有专门针对暗网的监管条例。

新加坡网络安全专家林福存表示：“你需要很多人力资源、专家、时间和金钱去管制暗网。而互联网本应该是全球使用、无国界的，如果需要跨国合作就更艰难了。不过除非有特定情况，例如毒品、武器或人口走私，政府才会针对性地进行调查、执法，而非制定通则，至少目前不会。”

由于难以追踪，暗网对黑客和不法之徒尤其具有吸引力。新加坡网络安全局就指出，暗网当中大部分的内容和服务都是非法的，包括提供黑客服务。当局劝请公众保持警惕，防范网络罪案。

 相关标签 [暗网](#) [darknet](#) [科技一点通](#)


### 头条新闻

- 
 新加坡 · 2019冠状病毒  
本地新增病例回落 报3472起  
21/04/2022 10:52
- 
 路车急停公路社院 幸无人受伤  
21/04/2022 10:52
- 
 新闻深呼吸 · 放眼天下  
晨光|着眼天下：各国如何以创新方式减少...  
21/04/2022 10:50
- 
 新加坡  
本地摊主歇业一周发难 默通告 惹笑网民  
21/04/2022 10:29
- 
 新加坡  
幼童爬树顶 “耍杂技” 倒着睡 网民猜测暗娼...  
21/04/2022 00:08
- 
 新闻深呼吸 · 律法知新  
狮城有约 | 律法知新：什么是合理的自我...  
21/04/2022 11:00