

ADVERTISEMENT

Uniquely exposed: How ultra-high net worth individuals are targeted by cyber crimes

'UHNWIs also have to be conscious that attacks against them can originate through their professional advisers'

Daniel Gore

06 August 2025 • 4 min read

SHARE



Hello and Welcome to the Professional Adviser Help Desk.



Criminals are becoming more experienced and skilled at social engineering techniques which can develop a digital clone of UHNWIs, writes lawyer Daniel Gore

Ultra-High Net Worth individuals (UHNWI) are increasingly becoming targets of sophisticated criminal attacks using a range of different methods.

Whilst physical attacks, such as kidnappings and burglaries, are still methods employed by criminals to attack UHNWIs and their families, cyberattacks have become an equal or, perhaps, greater focus due to the increased reliance on technology to operate and manage personal lives and commercial activity.

The practical reality is that it is easier for individual perpetrators or criminal organisations to target UHNWIs from a location thousands of miles away, rather than having to plan and coordinate a physical attack and then deal with the assets (which are often unique and identifiable).

UHNWIs are often high-profile figures so some of their personal information ends up being available online across different platforms and sources.

Even the most basic information about an individual can help criminals to form a digital personality, mimicking an UHNWI, or to ascertain their patterns of behaviour.

Criminals are becoming more experienced and skilled at social engineering techniques which can develop a digital clone of the UHNWI and, ultimately, lead to the manipulation of the UHNWI's contacts to obtain information about, or access to, their assets.

Rising risk levels

The risks of these types of attacks has significantly increased due to the globalisation of the corporate world and the behaviour of UHNWIs across their personal and business lives.

ADVERTISEMENT

UHNWIs often spend less time in a physical home or office location, instead choosing to move around the globe. That means they regularly engage in sensitive personal or commercial activity from unconventional environments. Joining board meetings from the deck of a private yacht, or leading sensitive negotiations from a seat on a private plane can increase the vulnerability of a UHNWI's data and technology. Engaging with personal bankers or financial advisers across different platforms and networks inherently exposes the communications to attack.

UHNWIs also have to be conscious that attacks against them can originate through their professional advisers.

Those professional advisors often hold a significant amount of personal information and details about assets. Criminal organisations can obtain access to the information held by professional advisors and deploy that data against the end clients directly, rather than engaging in an attack against the professional advisors themselves.

Traditional cyber attacks through email systems and messages remain a common form of cyber attack and continue to result in successful attacks against individuals and corporate entities. 'Phishing' attacks have evolved to become highly sophisticated and realistic, and where UHNWIs conduct business on their mobile devices (phones, tables etc.) the key identifiers of a scam email can often be obscured. 'Whaling / Whale phishing' is now a common form of that type of cyber attack which specifically targets UHNWIs.

Session hijacking is another method being adopted by criminals and this is particularly relevant for UHNWIs who conduct sensitive business activity remotely, often in unfamiliar surroundings where they do not have complete control over the security environment. This type of attack can expose both the individual and any corporate entity to damage, as the attacker can mimic the UHNWI and give instructions and commands.

Eavesdropping attacks (sometimes referred to as snooping or sniffing) are another risk for a UHNWI and can be particularly acute where the individual is operating across multiple devices on a regular basis, or moving between different data networks and communication platforms.

Corporations

Whilst the UHNWI should be focused on their own personal position, they also have to be conscious of the risks to which they also expose other people and corporate entities.

Cyberattacks regularly target corporate entities (and government infrastructure and organisations) and they are often successful due to the behaviour of a single individual. Whilst any individual in the corporate environment can be a target, the UHNWI is likely to hold a senior role and have access to much more sensitive information and systems.

The UHNWI can also inadvertently expose their own physical or digital assets. Digital records could be manipulated to alter the ownership details of a plane or yacht, which could then be sold on by the criminal to an unsuspecting third party. It may also be possible for criminals to divert the transport of artwork to themselves or to insert false credentials to gain access to secure storage facilities. Digital currencies can also be targeted, especially where possession of a unique key or code is the only means of identifying the owner.

Where a UHNWI does become a victim of a cyberattack, they should be conscious of their own legal liability in the circumstances. Should they inadvertently disclose information about a third party or business then there could be legal issues around money laundering and financial crimes, as well as data handling and reputational issues.

ADVERTISEMENT

The 'failure to prevent fraud' offence introduced under the Economic Crime and Corporate Transparency Act 2023 relates to corporate entities, but where an UHNWI's personal and business activities overlap, they may have to show that they have complied with the reasonable procedures put in place by their business(s) or they could risk breaching those provisions on behalf of the business.

In a crisis, it is critically important to have your trusted team in place to respond immediately and efficiently.

Daniel Gore is senior associate in Withers' litigation team

SHARE

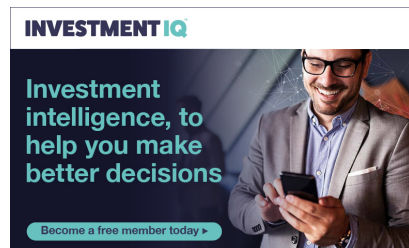


Related Topics

[Your profession](#) | [Daniel Gore](#) | [Withers](#) | [opinion](#)

PREVIOUS ARTICLE
Quilter reports
£4.5bn core net
inflows and adviser
growth

NEXT ARTICLE
L&G H1 profits rise
9% as CEO hails
'excellent six
months'



INVESTMENT IQ

Enjoy leading content from across the investment industry all in one place

Read on to find out

Sponsored by Investment IQ

ADVERTISEMENT

ADVERTISEMENT

More on Your profession



ADVERTISEMENT

YOUR PROFESSION

Aviva scraps final additional charge on adviser platform to offer single, transparent fee

Move to remove ETI charges aligns with Consumer Duty



Sahar Nazir

🕒 06 August 2025 • 2 min read



YOUR PROFESSION

L&G H1 profits rise 9% as CEO hails 'excellent six months'

ADVERTISEMENT
Growth from workplace pensions, annuities, and asset management



Sahar Nazir

06 August 2025 • 2 min read



YOUR PROFESSION

Uniquely exposed: How ultra-high net worth individuals are targeted by cyber crimes

'UHNWIs also have to be conscious that attacks against them can originate through their professional advisers'

Daniel Gore

06 August 2025 • 4 min read

Most read

01

Next Generation Advisers: Meet Succession Wealth's Rob Earle

06 August 2025 • 3 min read

02

Quilter reports £4.5bn core net inflows and adviser growth

06 August 2025 • 3 min read

03

Aviva scraps final additional charge on adviser platform to offer single, transparent fee

06 August 2025 • 2 min read

04

Phillip Wickenden: Frozen thresholds and the art of distraction

07 August 2025 • 5 min read

05

AI in financial services: Hype, hope, or a bit of both?

ADVERTISEMENT
06 August 2025 • 4 min read

06

Octopus Money to buy Virgin Money's investment arm

06 August 2025 • 2 min read

In-depth



YOUR PROFESSION

Polling high – should advisers bank on Reform UK holding on?

Nigel Farage-led party's policies would likely mean big tax changes if Reform came into power



Isabel Baxter

30 July 2025 • 7 min read

**YOUR PROFESSION****Financial planning 'badly' needed PFS £1m talent pledge – what next?**

Considerations include representation, showing not telling, and small business support



Jen Frost

29 July 2025 • 6 min read

**TECHNOLOGY**

ChatGPT is changing how clients find advisers

Prospective clients using AI tools to find financial advisers

ADVERTISEMENT



Sahar Nazir

17 July 2025 • 6 min read

Contact Us

Marketing Solutions

About Incisive Media

Privacy Settings

Careers

Terms & Conditions

Policies

FOLLOW US



© Incisive Business Media Limited, Published by Incisive Business Media Limited, New London House, 172 Drury Lane, London WC2B 5QR. Registered in England and Wales with company registration number 09178013. Part of Arc network, www.arc-network.com

DIGITAL PUBLISHER OF THE YEAR

