Protecting personal investors on UK investment platforms from cyber threats

Authors
Gerard Phillips, MSc (Royal Holloway, 2020)
Geraint Price, ISG, Royal Holloway

Abstract

The cyber-security of personal investors in the UK who use UK investment platforms to manage their pensions or savings is not well understood and not often discussed. Here we ask "What are the principal cyber threats to investors' assets on UK investment platforms and what can be done to prevent or mitigate these threats?"

To put the research in context this article summarises first how a growing number of personal investors are being 'pushed' online to use new and emerging technologies to manage their finances. Investment platforms are the technology of choice. It then outlines the development of a maturing criminal economy that is well-positioned to attack personal investors in this evolving sector. Cyber theft from personal investors should be expected to increase but are investment platforms prepared for such attacks?

Cyber-security professionals typically use strategic and operational threat intelligence models to make sense of (and thus prevent or mitigate) cyber attacks. This research demonstrates that existing threat models are inadequate to meet the new threats facing personal investors.

Using new synthesised real-world attack data, a new threat model is developed which focusses specifically on the risks to individual investors, not solely on the risks to investment platforms or banks. This allows us first to offer some new insights into actual attacks on investors. Second, it provides a new threat intelligence capability to anticipate and defend against future attacks. [a]

[a] This article is published online by Computer Weekly as part of the 2021 Royal Holloway information security thesis series https://www.computerweekly.com/ehandbook/Royal-Holloway-Protecting-investors-from-cyber-threats. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

Investors and investment platforms make attractive targets for cyber criminals

If you have a pension, or savings or investments, then it is increasingly likely that you (or your financial advisor) are using an investment platform to manage your money. Have you considered how safe these digital platforms, and your savings or pension accounts, are from cyber-crime?

Individual investors cumulatively contribute billions of pounds in investments to the UK economy. They are a significant part of the financial services sector which itself is part of the country's critical national infrastructure. Investors might trade in stocks or shares through online accounts, save using financial products such as Individual Savings Accounts (ISAs), or build a personal pension, for example through defined contributions pension schemes or Self-Invested Personal Pensions (SIPPs).

Three important sets of changes affecting investors are taking place: first, the sums being invested by individual investors are increasing (the growth of personal pensions offers one example). Second, investors increasingly are being 'pushed online' in order to manage their investments. (See for example the report *FCA Sector Views 2020* by the UK's Financial Conduct Authority.) Third, an increasing numbers of investors are using investment platforms to manage their portfolios. These trends can be expected to continue and together they offer a lucrative target to cyber criminals. What can be done to protect investors using investment platforms?

Investment platforms (sometimes called fund supermarkets) broadly are digital exchanges which allow you, as an individual, to invest in stock markets across the world. From your front room you can go onto your web browser and buy and sell shares in companies or commodities. You can invest in complex financial products such as Exchange Traded Funds and even day-trade using derivatives on platforms like eToro.

A general point to make is that investment platforms and banks differ markedly in the security they offer *personal investors*. Very roughly, more traditional banks have stronger identity and access management (IDaM) measures in place than some of the more recent, digital platform only companies. Platforms using hard tokens for second factor authentication for example offer greater protection than others which allow only a username, three digits from your password and your place of birth to access the account (these are real examples, specific platform names are withheld). This increasingly matters where insurance companies refuse to underwrite investment platform losses from fraud where it is the personal investor who has been deceived (through phishing, vishing or smishing for example), as distinct from a clear failure of the investment platform's security (e.g., through some hack).

This matters all the more for the current, older, generation of investors who are not generally 'tech-savvy'. A survey[1] was done which asked a cross section of investors what they knew about their online security for the investment platforms they used. The survey tested to what extent cyber guidance for investors (taken from the web page of a well-known investment platform) was actually understood by the respondents. It found investors have a limited understanding of the risks to them using investment platforms. If anything, they rely on others (the investment platform, the device manufacturer, software developer etc.) to keep them somehow safe.

So there are - and will continue to be - more personal investors, with more money held across more digital investment platforms, the security of which, for personal investors, is variable. But would this really matter so much, unless of course there is a credible threat to these assets?

Cyber-crime will continue to grow and evolve

In addition to the increasing potential rewards for crime, the technical opportunities for hacking financial services sector companies and investment accounts are increasing. At the same time the capabilities and organisation of criminals to conduct attacks is also improving. Figure 1 illustrates how these elements can combine to shape a modern threat landscape.

Three features stand out. The first point, simply, is that the more complex and interconnected systems become the more likely there will be vulnerabilities in the design, implementation or configuration of such systems. Second, a criminal ecosystem or 'marketplace' is now well established to support a high level of differentiation in cyber-attacks. Third, less sophisticated criminals now have access to better tools and a network of services to enable (or commission) more complex attacks. No one person needs to have all the technical knowledge or skills needed to conduct an attack.

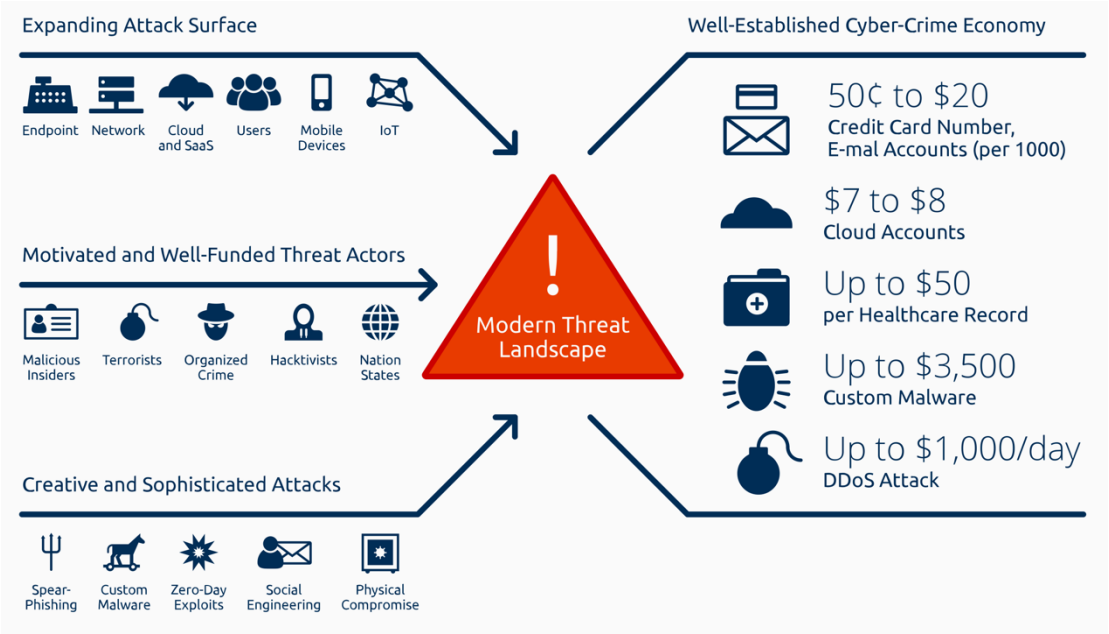
Taken together, these ways of working and cooperating extend the capabilities of criminals at both the lower and higher ends of the skills continuum. The lowering of a technical 'bar to entry' could also result in an increase in the numbers of criminals undertaking attacks.

How robust are UK Financial Services Sector (FSS) companies against such threats? Unfortunately, available evidence from the FCA, analysed in the research, suggests that the capability of UK FSS institutions to protect themselves from cyber attacks appears highly variable and in some cases below industry standards (e.g. the ISO27000 family). At the same time available UK data on cyber attacks on financial services (while partial) shows a general increase in attacks across all UK finance sectors. These include the 'Pension Savings & Retirement Income' and 'Retail Investments' sectors where personal investors are typically most active.

It is reasonable to expect that the degree of differentiation across the criminal community, combined with a sophisticated marketplace in capabilities for sale, could therefore lead to a focussed and sus-

[1] See the full dissertation, available at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

Figure 1: A Modern Threat Landscape 2020



Source: "Threats Have Evolved–Has Your Security Program?" [Online]. Available: `https://www.siemworks.com/Solutions-Security.asp`. [Accessed: 13-Aug-2020].

tained assault on personal investor accounts. Nearly 10 years ago Operation High Roller did just this, the focus being then on high-balance bank accounts in Europe. (It targeted between €60 million and €2 billion using a customized Trojan spyware tool.)

Understanding cyber attacks across the Financial Services Sector

How best can cyber-security professionals make sense of (and thus prevent or mitigate) attacks on investment platforms? A 'top-down' approach is to use threat modelling. This is generally straightforward:

1. Find a relevant threat model that can best explain what the threat is, to whom and from whom. In our case, that is theft from criminals hacking investor accounts on investment platforms;
2. Populate the model with the best quality available real-world data of known attacks on your targets;
3. Using this real-world attack data, develop a series of strategic threat models detailing possible attacks. From this one should get a decent understanding of the extent and nature of the exposure of your 'targets' to different cyber-attacks. One scenario for example could examine attacks on APIs that share credentials and personal finance data across different institutions (a consequence of the recent Open Banking and Open Finance initiatives);
4. Detail and work through specific attack scenarios. This gives you your operational threat models. Understand the exploits (i.e., the specific steps taken by an attacker to compromise your system) and then develop prevention and mitigation measures. MITRE ATT&CK tactics, techniques and procedures (or some equivalent) should be used to detail each scenario. For example, the *DefensorID Mobile Banking Trojan* was a real attack that could steal from a wide range of accounts including cryptocurrency wallets. For this scenario one would script for each attack vector the procedures for prevention and mitigation;

5. From such strategic and operational scenarios an organisation could then concentrate its resources on the more likely attacks and ensure it has the capability and capacity for an immediate tactical threat response should the attack(s) occur.

Identifying cyber attacks on individual investors

No threat model was found in our research that allowed us to understand attacks on personal investors on investment platforms. Nor was UK-specific real-world attack data on investment platforms available. This research therefore developed a new threat model and populated it with real-world attack data synthesised from existing datasets. There were two outcomes: first, it offers a series of new insights into actual attacks on investors. Second, it provides a model to anticipate, and prepare for, future attacks.

Creating a new threat model

An immediate challenge for the research was the absence of a relevant threat model to adopt. Typically most analyses of attacks in the financial services sector focus on 'financial institutions'. However, a sole focus on 'institutions' has two limitations. First, it effectively ignores the central position of individual investors as targets for cyber theft. Second, it does not provide sufficient granularity in distinguishing between significantly different types of institutions.

Consequently this research created a new model and defined three distinct 'threat landscapes' as follows:

- By **investor landscape** we take to mean the setting of individual investors who use applications and devices to make transactions on investment platforms. Currently this would typically be via a website or an app on a computer, tablet or mobile;
- The **institution landscape** comprises companies that are 'customer facing' and are typically regulated by the FCA, such as investment platforms, retail banks, lending and investments, pensions and investment management companies etc.;
- The **infrastructure landscape** could be more broadly defined to include the companies, services or institutions that support and enable FSS institutions to trade, such as clearing banks, payment systems and exchanges.

This is important because different landscapes can have different attack surfaces, that is, opportunities for attackers to exploit vulnerabilities. For example, an attack on an investor managing their finances at home on their desktop or mobile device presents a very different challenge from an attack on an institution such as a bank or an investment platform, which needs to consider the security of its devices, applications, networks, data and personnel across a far wider geography. Similarly, attacks on payments and inter-banking systems (such as SWIFT) use different attack vectors and threat events to an attack on a bank.

Finding relevant attack data

A second (and unexpected) challenge in trying to understand cyber attacks across the financial services sector in the UK proved to be finding the relevant data with which to test the threat models.

Both the Financial Conduct Authority (FCA) and the UK National Cyber Security Centre (NCSC) collect UK relevant data. The FCA legally requires of the (at least) 59,000 companies it regulates that they must report a cyber incident to it if is deemed "material" under Principal 11 of the FCA handbook. The NCSC collects data through several means, not least through the intelligence sharing arrangement, the Cyber Security Information Sharing Partnership (CiSP). Unfortunately, neither would make any data (not already in the public domain) available for the research.

The solution to this difficulty was to synthesise a new dataset from two sources:

- the excellent Carnegie Endowment for International Peace dataset on global financial cyber attacks (curated by the Cyber Threat Intelligence Unit of BAE Systems (British Aerospace Engineering)[2]; and
- the informative dataset on the "Information is Beautiful" website[3], filtered for financial attacks.

This resulted in the creation of a unique dataset (detailed in Appendix 1 of the full dissertation) of 153 major cyber attacks across the financial services sector worldwide from 2005 to 2020. (To note, the lack of appropriately detailed attacks on UK investment platforms meant some assumptions were made to allow us to draw inferences from the dataset to UK investment platforms.)

Major attacks on the Financial Services Sector and on individual investor accounts

Using this new data with new threat models brings new insight into the threats facing investors. For the first time it becomes clear (see Table 1) how significant a target individual investors really are: 12% of all attacks were, principally, attacks on investors. Specifically, the *focal point* of the attack was on individual personal accounts, not on the FSS institution.

Table 1: Diversity of Threat Landscapes

Threat Landscape	#	% (rounded)
Investor	18	12%
FSS Institution(s)	90	58%
FSS Infrastructure	45	30%
Total	*153*	*100%*

What also stands out from the data is how much remains unknown; in many cases years after the attacks are over. For nearly half (47%) of all attacks (see Table 2) we can't say, even broadly, who the attacker really was.

Table 2: Types of Threat Actors by Threat Landscape

	State-sponsored	Non-state actor	Unknown	Totals
Investor	0	9	9	18
FSS Institution(s)	17	34	39	90
FSS Infrastructure	11	11	23	45
Threat landscape total	*27 (18%)*	*54 (35%)*	*71 (47%)*	*153 (100%)*

Nor do we know how nearly a third (31%) of attacks were actually carried out. From the data available, it appears that newer attacks are not necessarily using more complex tools, but that there is an increasing capability to use existing tools in new ways. For example, attacks by APT Group 41 use common network commands such as ping, FTP and pwdump alongside the more traditional Cobalt Strike and China Chopper malware exploits. Overall, the use of multiple attack vectors was the fourth most popular means of attacking targets.

[2] "Timeline of Cyber Incidents Involving Financial Institutions." [Online]. Available: `https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide` [Accessed: 25-June-2020].

[3] `https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/` [Accessed: 14-Aug-2020].

Recommendations

The key points for **individual investors** are:

- The data shows they are at risk:
  - Over 10% of all attacks targeted individual investors, generally personal customer accounts. The motivation for almost all attacks against personal investors is theft;
  - They are carried out by organised criminal gangs (i.e., non-state actors), mostly working from Eastern Europe;
  - The principal attack vectors are malware, forms of card theft and "multiple" vector attacks;
  - The fact we still don't know technically how many of the attacks were carried out or by whom limits any conclusions we might draw but suggests that the criminals are one step ahead of everyone else;
- Investors should begin to expect, and insist, that investment platforms provide good quality data that demonstrate how secure their platforms are compared to their competitors. Investment platforms typically publish comparative data so consumers can decide which is the best platform for them, such as the cost per trade, markets that can be accessed, research tools available etc. Why not do the same for the cyber-security of a platform? Does ISO 27015 provide a starting point?

For **investment platforms** and **banks**:

- Conventional threat models are inadequate because they are designed to protect the financial institution and not investors. Both strategic and operational threat models need to be developed for the investors' threat landscape. A practical step financial platforms and banks could take to better prevent or mitigate attacks is to develop relevant threat model scenarios. This research details a number of likely attack scenarios;
- Investing resources that defend against known or probable attack scenarios is self-evidently a better use of resources than any 'hit and hope' defence strategy. If you misunderstand the threats you and your customers face, the chances are also you will be the less secure for it;
- Investor security must become a stronger priority. Put simply, make two factor authentication (2FA) mandatory and use hard tokens. At a push, use Yubikey if you don't have your own. It just does not make sense that lower value accounts (such as some day-to-day bank accounts) have better security than some very high value accounts held on investment platforms (which if it holds a pension, can well be in excess of £1 million). Just to note, the criminal gang who ran Operation High Roller as long ago as 2012 managed to bypass the 2FA in place at the time to perpetrate their fraud;
- Investment platforms could also be more proactive in helping their customers protect themselves. Simply publishing a page deep in your website somewhere about how individuals should be responsible for their security (advice on phishing for example) is unlikely to achieve much. The point is to help customers develop safer online behaviours. Barclays 'Digital Eagles' initiative provides a practical example of what can be done;
- Publish an industry-standard benchmark so customers can decide for themselves if your site is secure to use or not. (A re-working of ISO27015?)

For the **Financial Conduct Authority** and the **National Cyber Security Centre**:

- One remit for the FCA is to protect consumers. One objective for the NCSC is to protect our critical national infrastructure. Protecting investors should be an important priority for both organisations;
- For future research it would be most helpful if they would publish or share data to enable more detailed research into the specific threats faced by UK investors. Commercial sensitivities and confidentiality can be managed, for example through aggregation and/or anonymisation of data.

Conclusion

Individual investors will increasingly become targets for cyber criminals. Investment platforms (and similar platforms which hold investment or trading accounts) need to develop their strategic and operational threat intelligence to better protect investors. This applies especially, but not exclusively, to the growing numbers of less tech-savvy older and more vulnerable members of society who have pensions or savings to protect.

Biographies

Gerard Phillips is a 2020 graduate of Royal Holloway College. He has used a number of investment platforms for around 20 years. His particular interests are in the area of threat intelligence and penetration testing in the FinTech and Investment sectors. Gerard can be contacted on gpcybersec@gmail.com. His LinkedIn profile is www.linkedin.com/in/gerarddphillips.

Geraint Price is a Senior Lecturer in Information Security. A key part of his activity within the Information Security Group (ISG) is to engage with leading international information security organisations. This involves representing the ISG in several industrial forums, including: ISF (Information Security Forum), and I-4 (International Information Integrity Institute). He is also an elected member of the Management Committee for IAAC (the Information Assurance Advisory Council).

Series editor: S.- L. Ng