

Corporate Learning Pulse

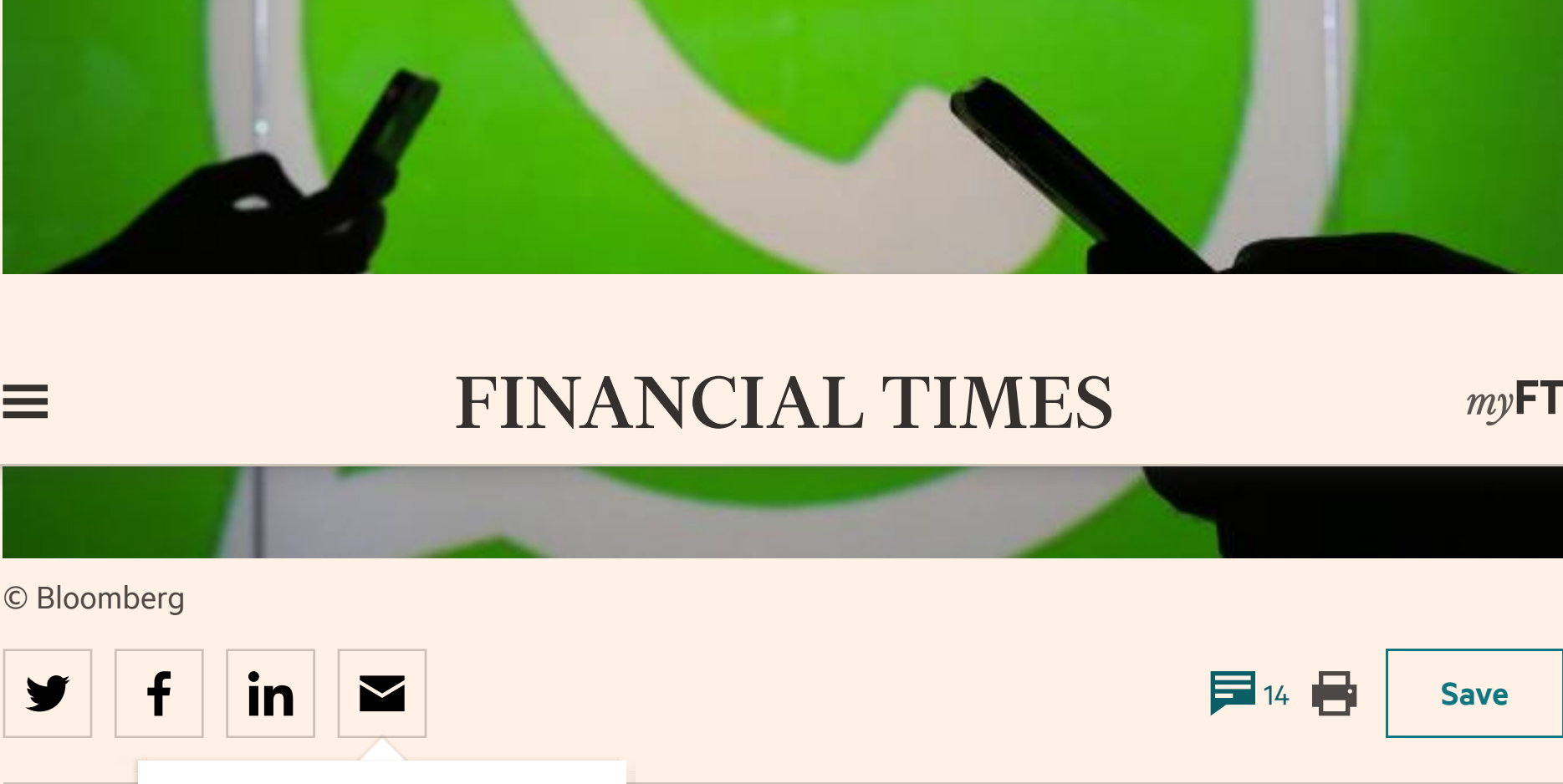
Unique survey of 600 business leaders across Europe reveals attitudes on investment in people

Insider Trading

+ myFT

Insider trading schemes using encrypted apps alarm FBI

Self-destructing messages are the latest tool for white collar criminals



© Bloomberg



14

Save

Subscribers can gift articles

The Federal Bureau of Investigation is growing concerned that Wall Street traders are turning to encrypted apps to hide illicit communications from internal compliance programmes and regulators.

Encryption is “a growing problem overall,” John Casale, an assistant special agent in charge of complex financial crimes in the Manhattan field office told the FT. “New technology comes out and you know it’s going to be applied and it could be applied in a way to engage in fraud, money laundering, and insider trading.”

The first indication that applications, such as WhatsApp, Signal or Telegram that allow for secure end-to-end communications, are being used by white collar offenders inside big banks came to light late Wednesday in a largely unnoticed insider trading case.

Advertisement

howtospendit.com

PAID POST BY MYLISSE HARDIN



Savoir-faire in motion: the exquisite jaquemarts

A former IT employee with [Bank of America](#) pleaded guilty to a wide-ranging insider trading scheme that netted over \$5m in proceeds, according to civil and criminal charges brought by the Securities and Exchange Commission and US attorney’s office in Manhattan.

Daniel Rivas, the former bank employee, used a phone messaging app to pass encrypted, self-destructing messages to three friends about confidential corporate takeovers, according to the SEC [complaint](#).

FBI agents say white collar criminals are adapting, whether it’s moving from group communications on Bloomberg chat rooms to social media pages like Facebook that fall outside of traditional business communications platforms, or touting stocks on popular platforms like Instagram.

Encrypted devices and phone apps have been an obstacle for agents tracking terrorists who “go dark” to evade surveillance — an issue that has raised concerns about civil liberties and privacy and resulted in a showdown with technology companies.

The shift to new technologies is not unexpected. Pre-paid cell phones, known as burner phones, were used in the insider trading case involving sports bettor Billy Walters and Tom Davis, the former chairman of Dean Foods. Encrypted text messages were used in a 2016 stock promoting case.

In March, the UK’s Financial Conduct Authority fined a Jefferies banker £37,198 for sharing confidential information on WhatsApp — the first action of its kind.

Marten den Haring, chief product officer of Digital Reasoning, an artificial intelligence-based computing platform that some financial institutions are using for surveillance, says, “People are starting to get creative and using some of those communication channels that are harder for law enforcement and internal teams to lay their hands on.”

The evolution is reflected in Digital Reasoning’s own history. It was adopted early on by the US Department of Defence to track suspected terrorists. Beginning in 2012, its analytics started to attract Wall Street firms’ interest. [Goldman Sachs](#) became an investor and client.

Mr den Haring says its software can use behavioural patterns to detect when people want to change communication channels so even if their communication goes offline it leaves “breadcrumbs” behind.

“All these breadcrumbs when put in proper order and context can give you clues to act on. That’s the race that everybody’s in. My only worry is: can the government adapt fast enough?”

Copyright The Financial Times Limited 2017. All rights reserved. You may share using our article tools. Please don't copy articles from FT.com and redistribute by email or post to the web.



14

Save

Latest on Insider Trading

FT Alphaville

Alexandra Scaggs

Reminder: Your “self-destructing” messages do not actually self-destruct



Insider Trading

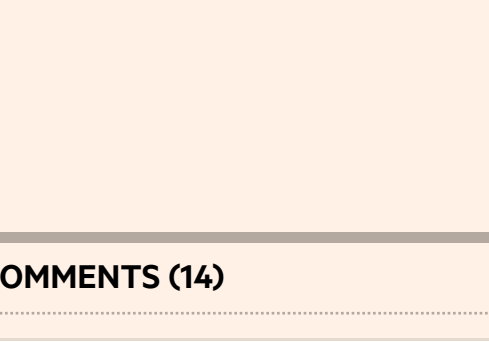
Walters sentenced to 5 years for insider trading

Prison term for ‘brazen’ \$45m scheme handed down in spite of high-profile testimonials

fastFT

Sports gambler Billy Walters sentenced to 5 years for insider-trading conviction

Paid Post



Paid Post by Rambus

What the Spanish flu pandemic can teach us about cyber security

The parallels with the growing threat of a cyber pandemic offer preventative insights


Latest in Financials

Financial & markets regulation

UK banks plan for new rules on bad loans

Survey reports some will have to increase provisions for bad loans by up to 25%

NEW AN HOUR AGO



The QE retreat

ECB faces bond shortage as inflation slows

Traders will scrutinise a gathering of central bankers at Jackson Hole for policy signals

NEW AN HOUR AGO

Financial Services

P2P student fee lender secures \$240m for US push

Prodigy obtains debt and equity funding as it targets foreign postgraduate students

myFT

Follow the topics mentioned in this article

Financials	+ myFT
Markets	✓ myFT
Federal Bureau of Investigation	+ myFT
Companies	✓ myFT
Banks	+ myFT

Follow the authors of this article

Kara Scannell	+ myFT
---------------	--------

[Take a tour of myFT](#)

COMMENTS (14)

AnotherMexAbroad 6 hours ago

Hardly surprising this is going on. Even more obvious is that governments will attempt to fine / legislate / regulate.

Report Recommend Reply

Winston smith 7 hours ago

@spaceTime. indeed, those channels are secure for the time being. they are also mainstream, there are other routes that are less obvious and more secure. there are, however, other ways of tracking people who converse on secure media. pattern analysis, for example: it is relatively easy to identify individuals from the pattern of their written text.

as for the monitoring of trader comms, secure apps are no more 'out of band' than chats down the pub...

Report 1 Recommend Reply

Spacetime 6 hours ago

People focus on encryption itself. Do you see your encrypted message on your screen? Are you the only one who sees it? And we are not talking about surveillance cameras in case you jump to the wrong conclusion.

Report 1 Recommend Reply

UKAthiest 6 hours ago

This is the biggest risk, indeed.

Countries (especially the USA) are pushing for 'back-doors' to be installed into software so that they may be accessed if law enforcement sees fit..

The problem with this, is that you significantly reduce the efficacy of the encryption itself, and is open to myriad abuses - it is thus facing serious push-back from the tech industries.

A good article on this from FT: <https://www.ft.com/content/8c8de3b8-12d0-11e7-80f4-13e067d5072c>

Report Recommend Reply

Spacetime 5 hours ago

@UKAthiest Pushing for back-doors as a recent phenomenon or they already have staff inside those companies that provide them with special services since pre-smartphone times? If both powerful businessmen and politicians can be pushed to do anything by secret services then surely IT stars ought to be a walkover.

Report 1 Recommend Reply

JP 7 hours ago

Oh any surprise that now bbg and company chat is monitored like a hawk traders turn to whatsapp and other encryption? I know personal phones are now outlawed many floors ... but it just drives this underground...

Report Recommend Reply

UKAthiest 8 hours ago

Poor FBI - they may as well complain that the Sun rises in the East!

Encryption is a mathematical tool that cannot be wished or legislated away!

Report 1 Recommend Reply

Spacetime 9 hours ago

Whatsapp, Telegram, and Signal are all surveillance - free? Please.

Report 2 Recommend Reply

UKAthiest 8 hours ago

@Spacetime Sorry, but you clearly know very little about how encryption actually works.

You can 'survey' all the encrypted messages you like - without the encryption key, your chance of deciphering said messages is round about a big fat 0.

Report 2 Recommend Reply

Spacetime 8 hours ago

One day you will remember this little piece of confident chit chat. When that day comes, I recommend you asking yourself the following 'what else am I so certain about today as I was sure of back then?

Report 2 Recommend Reply

UKAthiest 7 hours ago

@Spacetime You're right - one day! That day is when we have working quantum computers.

I'm about as cynical as you can get, but that day is not now - the ability to break 256-bit or higher encryption simply does not exist currently.

For example, let us take a smaller, easier 128-bit AES key - this has a total of 13.4 x 10^38 combinations, and would take the world's most powerful supercomputer (circa 100 Petaflops) over 100 trillion years to 'brute force' a solution to this encryption. Seeing as the universe is circa. 15 billion years old...

Tens of Trillions of Dollars/Euros/Whatever are securely traded around the world thanks to encryption every day - the same encryption these pesky bankers are using.

When Quantum Computers arrive? Well, cryptographers & mathematicians are already working on quantum-proof techniques - the most promising of which is lattice-based cryptography.

Maths does not lie - the FBI (and Amber Rudd for that matter) may as well proverbial into the wind for all it matters.

Report 2 Recommend Reply

+ 3 replies

Show more comments

Tools

Portfolio

Today's Newspaper (ePa...

Alerts Hub

Lexicon

MBA Rankings

Economic Calendar

News feed

Newsletters

Currency Converter

More from the FT Group

Markets data delayed by at least 15 minutes. © THE FINANCIAL TIMES LTD 2017. FT and 'Financial Times' are trademarks of The Financial Times Ltd.

The Financial Times and its journalism are subject to a self-regulation regime under the FT Editorial Code of Practice.

A Nikkei Company