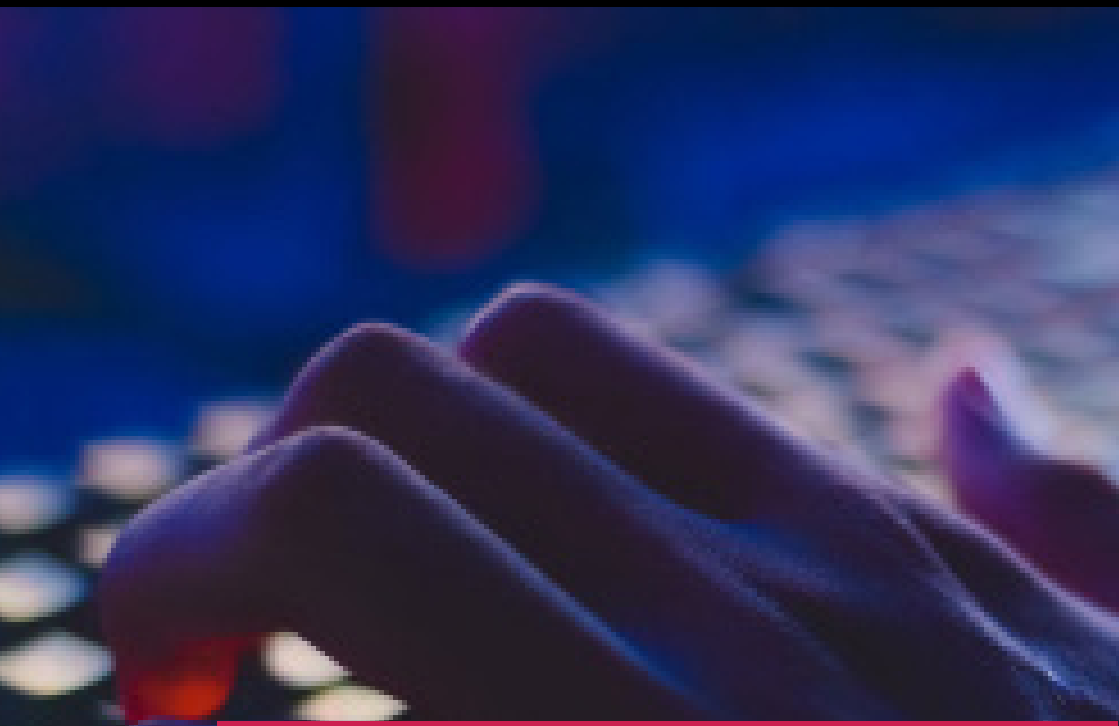
wiztrust



CORPORATE NEWS HACKING AND FINANCIAL HOAXES

Innovative Solutions to Face Emerging Risks

Certified with wiztrust

TABLE OF CONTENTS

FOREWORD

Many companies and mainstream media outlets are facing a new challenge. How to ensure trust in an era of social media, artificial content creation, and fake news? Publicly listed companies and financial institutions worldwide are the most exposed to rising threats.

The content of financial and business communication directly impacts the value of the companies involved. Fictitious articles and fabricated news campaigns create harmful effects not only on a company's reputation but also on their financial stability. In 2016, a fake press release was directed at one of the largest construction companies in the world, Vinci. The article sent its stock crashing nearly 20%. In just 7 minutes, more than $7.4 billion had vanished from Vinci's market cap.

There are numerous ways to manipulate corporate and financial information. In this white paper, we assess their level of sophistication, from a simple press release to elaborate schemes to gain access to well-protected IT systems. When it comes to finding loopholes for profit, the imagination and the ingenuity of hackers are limitless.

The authors of those attacks not only have numerous techniques, their actions follow various motives. Some are novice or seasoned hacktivists trying to raise awareness for their cause. Those hoaxes and pranks are some of the best tools in their influence arsenal.

The YesMen made a name for themselves after their most recent hoax. On January 16, 2019, The YesMen sent out a fake annual letter to investors and journalists signed by Larry Fink, CEO of BlackRock, hours before the release of the real annual letter. The fake letter proudly announced the world's leading asset manager would sell out its investments in the fossil fuel industry in compliance with the Paris Agreement. An astonishing pledge that managed to fool mainstream media outlets like the Financial Times and CNBC.

Other fraudsters use fake corporate communication to manipulate the market and use their prior knowledge of the hoax to engage in insider trading schemes. The gains generated by those sudden variations on the stock market can make them rich in minutes while being very difficult to trace.

An objective and factual analysis is essential to understand how to anticipate and better face these rising threats.

This white paper thus includes a list of actual hoaxes and fraudulent attacks that were covered by the media. Those use cases depict an accurate and realistic landscape of the various aspects of “corporate news hacking.”

Over the past decade and a half, Wiztopic’s team of experts have gathered numerous factual accounts of corporate hacks to design a solution as to how corporations and the media should protect their external communications. Those findings led Wiztopic to develop Wiztrust.

Headquartered in France, Wiztrust is the main certification and verification platform for all corporate information. Wiztrust harnesses the cryptographic power and immutability of blockchain technology to allow companies to certify their communications in just two clicks. Journalists, readers, and investors can then verify the integrity and authenticity of the financial information by dragging and dropping the content onto www.Wiztrust.com.

The recent innovations in the digital world disrupt the business of communication for better and for worse. This double-edged sword allows fake and real content to be spread at a rapid rate and is the crux to most corporate hoaxes. We believe that great innovations need to be adopted to fight the problems these innovations can bring.

Jérôme Lascombe et Raphaël Labbé

Co-founders of Wiztopic

REAL TIME INFORMATION, REAL TIME THREATS

The speed at which information is circulated is constantly accelerating. Business and financial media, especially public relations agencies and business wires, have little to no time to check the authenticity of a piece of news or press release. With the progress in artificial intelligence, an increasing volume of content is produced by bots that are publishing articles and briefs without any human verification.

With the rising levels of distrust towards journalists, the media is in a critical situation when they face highly sophisticated hacks with fake press releases. These are difficult to detect, especially when coupled with perfectly mirrored websites, realistically spoofed emails, and fake press releases. Checking an official-looking document becomes a time-consuming yet necessary task.

Nowadays, corporate communication is shared through multiple channels, via a press release sent through an official email address, a wire, a tweet, or in a newsroom on the company's official website. Unfortunately, when official communication responsibilities are scattered throughout several teams such as PR, social networks, digital, internal... achieving perfect synchronization becomes near impossible. Hackers have learned to take advantage of those little delays a journalist might overlook.

Our experts found that corporate information hackers have refined their methods since the first big hoaxes, 15 years ago, and now combine most if not all, those communication channels. A well-prepared attack often involves a fake press release sent through a fake yet similar email address, with a hyperlink sending the recipient to a spoofed newsroom on a mirrored website with a "typosquatted," hijacked URL. For the most elaborate attempts, those documents even include a phone number, leading to a corporate voicemail or answered by a fraudster pretending to be part of the PR team. In this case, even a trained and meticulous journalist might be fooled by the apparent confirmation of the fabricated news.

Verification is even more costly when it comes to important news. Having the scoop on such information, even for a couple of minutes, is both a matter of reputation and profit for the media company. Fraudsters and hacktivists exploit this urgency to deceive journalists into relaying apparently legitimate fake news on social media, and sometimes in reputable media with a wide audience.

Unsurprisingly, our inventory of use cases reveals that fraudsters and pranksters bait journalists with carefully crafted content to tease their thirst for a news exclusive. The fake press releases fall into two main, non-exclusive categories.

A substantial share of fraudulent communication materials sent out by fraudsters are about extraordinary, unpredictable events that would require urgent crisis communication. In a context of urgent response, a communication team might be more likely to commit minor blunders while a journalist rushing for the buzz might overlook those little discrepancies.

When they are not betting on the element of surprise, many fraudsters do exactly the opposite. In several cases, they sent spoofed press releases right before a very anticipated event or deadline, such as the publication of an annual letter to investors or of a company's financial results. Those attacks are taking advantage of the expectations of journalists and their finance-savvy audience. A press release covering a planned event or a recurrent communication landing in a journalist's inbox on the right day has greater chances to escape his scrutiny.

This verification work is even more critical since we have entered the era of 24/7 media. Any fake information shared by one media outlet, especially a reputable one, can be spread by many. This continuous propagation of information is amplified by social networks, where any news article, video, tweet or post from a journalist can be shared and commented on by thousands of people in a matter of minutes. Moreover, according to MIT researchers, in a study published in Science on March 9, 2018, fake news spreads even faster and wider than real information.

Social media are constantly on the lookout for the next trend that will emerge thanks to their algorithms. Companies can be formidable echo chambers for fake news. They might also be the catalyst of their effects. Investors are continually monitoring these networks to understand their sentiment and adapt their strategy as quickly as possible.

THE MOTIVES: ACTIVISM AND PROFIT

In most of the cases we listed, cyber-activism as well as greed are the motives behind corporate communication hacks.

Corporate communication hacking is a very useful tool for activists to gain media coverage for their cause. The manipulation of official information is also often a way to highlight one company's little-known controversial actions, to mock a brand, to damage a business' reputation, to influence its management or to call for a boycott. This is often referred to as simple "PR pranks" or "hoaxes."

Greed is also a powerful driver of corporate communication hacks. When the hoaxes are not the vessels of some social or political message, fraudsters try to influence and manipulate the market, benefiting from the sudden upward or downward slides produced by a breaking news only they could expect. This form of "induced" insider trading generally targets public companies of various sizes: from traditional pump & dump on penny stocks to complex schemes influencing some of the biggest names on the world's leading exchanges.

A pump and dump scheme is an attempt to profit off the temptation of an easy and quick profit in small marketplaces and exchanges with high volatility. A fraudster would first acquire a large number of cheap "penny stocks" in a small company before spreading fake or exaggerated positive news on the market to drive the stock price up and sell out those stocks at high price to more gullible investors, driven by the fear of missing out on a potential gold rush.

However, hackers may sometimes use this mechanism in the opposite way. A fraudster would first take bearish positions on an asset and spread negative news on the targeted company to artificially drive its value down. The wrongdoer could then buy back in, share a spoofed denial statement or wait for an official one to be issued in order to profit off the stock's recovery.

In both cases, gains can be quick and massive. The use of derivative products following a whole index or basket of assets and not just one company can make those fraudulent profits nearly untraceable.

Those market manipulation techniques attempting to influence the market are typically not new and they could also include more basic forms such as financial spamming through emails, fabricated newsletters, and fake forecasting. Nonetheless, new media habits and technologies as well as high-frequency trading considerably amplified and accelerated their effects. In a recent study dedicated to market manipulation and suspicious stock recommendations on social media, Sorbonne University's Thomas Renault found that: "Fraudsters trying to spread out fake news use primarily press releases (73.3%), emails or newsletters (34%), websites (32%) and forums (10.6%)."

THE RISKS: MINIMAL COSTS, LARGE CONSEQUENCES

The proliferation of corporate communication hacking cases might be partly explained by the asymmetry between the resources needed to undertake such operations and the potential gains of the fraudsters and the cost for the targeted company. Getting a fake press release published requires minimal resources in comparison with the potential backlash that the victim, its brand image and its valuation might suffer, especially since the authors of corporate communication hacks are rarely identified and arrested.

Some attacks, such as the impersonation of Larry Fink, CEO of BlackRock, with a spoofed letter to investors, will "only" damage, sometimes permanently, the brand a company built, making revelations to the public that, real or not, might destroy years of customer relationships, good PR and corporate social responsibility efforts. Others lead to much more quantifiable financial damages.

Back in 2016, after months of public scrutiny, pharmaceutical giant Pfizer was targeted by a fake press release claiming the company would no longer increase the prices on their top-selling drugs. This news was released the day before April Fool's day using a fake URL, "pfizerinternational.com", and a press release was sent to the media. The Washington Post was quick to break the news and issue their take. The goal for the hackers was to manipulate the stock price and make a quick profit by shorting the price. Thanks to early warnings by market analysis firms and the responsiveness of the company, Pfizer's stock only stumbled by 2% after the news.

French construction giant Vinci was not as fortunate. On November 22nd of the same year, a fake press release announced serious accounting mistakes in the last earnings report, resulting in the group's Financial Director's immediate firing. In the seven minutes following, Bloomberg and the Dow Jones published the news. Vinci lost $7.4 billion of market capitalization, before trading on its stock was halted. Then a fake rebuttal was issued (since the fraudster was probably trying to benefit from both the downfall and the rebound), and was followed by the official rebuttal. The company ended up losing 4% of its value in a single day.

Those losses highly contrast with the estimated costs of the hack. Sending a fake press release is free, making a mirror website of the official one can be learned in a short time, hosting it costs the hacker roughly $23, answering the fake phone number to impersonate a PR officer and confirm the news only requires a $5 prepaid phone card. Taking a high estimate, the total cost of the attack probably amounted $30.

Every single dollar spent by the hacker cost Vinci, at worst, 246 million dollars.

Finally, the judicial remedies are extremely limited. While the SEC and other financial regulators around the world can launch investigations, the odds of finding out the identity of the hacker or group of hackers are low. Instead, they end up issuing new guidelines with good practices that can only postpone the next big hack. However, while fact checking is becoming a more prominent part of media ethics, it would not be surprising to witness, in the near future, that companies targeted by fake news will turn against the media which legitimized the fake information and seek recompense for these damages.

Minimal risks, limited resources but maximal impact; corporate communication hacking is characteristic of the most recent cyber-crime techniques. It requires potential victims to preemptively adopt new behaviors and innovative tools in order to prevent risks that will only become greater and greater.

A MASSIVE NUMBER OF ATTACKS SINCE 2010

The 2000 Emulex hoax, when a Californian optic fiber manufacturer lost 62% of its stock value following a fake press release, is the first major corporate communication hack that garnered considerable public attention. Information manipulation techniques have rapidly evolved since then, and we decided to list here a selection of the most characteristic cases of corporate news hacking of the past decade. Some made it to the front page of the newspapers, especially when they were an activist endeavor to gain coverage. Others remained under most radars, handled as silently as possible to cover a hacker's tracks or to protect the target company from greater undesirable effects, like some financial manipulation cases.

2019

BLACKROCK

BlackRock and its CEO, Larry Fink, were targeted by an elaborate information manipulation scheme. Just a few hours prior to the publication of Larry Fink's traditional letter to investors, some news outlets were deceived by a fake letter, reportedly signed by the CEO, sent out via a fake email and backed by a fake website. In the letter, the author announced that the biggest asset manager in the world would transition away from any non-environmental-friendly investment. Reputable media sources such as the Financial Times and CNBC news covered the letter as real.

2016

VINCI

Vinci, one of the largest construction conglomerates, issued an alarming press release claiming, "serious accounting mistakes have been made resulting in the layoff of their Financial Director." Bloomberg took the fake press release and website seriously and broke the news. The stock plummeted 18% in only a few minutes before the trading was halted. Despite some activist claiming responsibility for the hack, the French financial markets regulator suspect the goal of the operation was the manipulation of Vinci's stock price, but never identified who benefited from it.

FITBIT

California startup Fitbit was the victim of a pump-and-dump scam orchestrated by Robert Walter Murray, a Virginia fraudster. Using the SEC regulatory filing database EDGAR, Robert Murray created a sham tender offer by a nonexistent Shanghai-based financial firm called "ABM Capital Ltd." According to the filing, ABM claimed to be ready to buy Fitbit stocks at a whopping 46% premium, for $12.5. Fitbit capitalization broke $100 million as its stock rose 8% as soon as the filing was made public. Robert Murray, who only made an outstanding profit of $3,914.08 from the scam, was sentenced to two years in prison.

2016

PFIZER

Just before April Fool's day, a press release claimed pharmaceutical company, Pfizer, would no longer increase its drug prices. After months of drug price deliberation, the recent fake news duped the Washington Post who was quick to report this timely reaction. Advisors were quick to warn investors the news was probably fake, but the latter had already shorted the stock, which fell 2% following the news.

2015

RYANAIR

Irish airline Ryanair is no stranger to spectacular PR stunts. So much so that several European newspapers helped Italian hacktivist group Luther Blissett create a buzz, by going along with a fake press release and a fake website announcing a fictitious operation titled "Ryanfair." Ryanair was, according to the document, to fly migrants and refugees from Greece and Eastern Europe towards Germany, France, Denmark, Spain and Italy to denounce the lack of action of those countries regarding the situation. Ryanair quickly brushed off the whole story as a hoax.

2014

G4S

G4S, the largest security services provider in the world, seemingly issued a press release, linking to a mirrored website, stating serious accounting errors and the subsequent firing of the CFO. Despite some basic grammatical mistakes and references to the name of the former CFO instead of the current one, a few journalists shared the news on social media, which was picked up by news channels. While newspapers such as the Telegraph immediately alerted G4S of the suspicious statement, the stock slipped by a few points before recovering at the end of the afternoon.

INTEL

After disclosing a $6 billion investment project in Israel, Intel fell victim to a serious hoax. An official-looking press release backed by a, spoofed Intel newsroom and phone number, announced that the IT company was halting its investment considering "Israel's recent assault on Gaza" was contradicting the firm's corporate citizenship guidelines. The author of the hoax even answered the phone to confirm the news to inquiring journalists.

2013

EUROPEAN INVESTMENT BANK

The European Investment Bank allegedly announced they would cut funding for any kind of coal-related activity, the day before the publication of its yearly financial report. The ecological activist team behind that PR prank even answered the phone number included in the fake press release, pretending to be an EIB

2013

SAMSUNG / FINGERPRINT CARDS

Thanks to a fake press release claiming its imminent acquisition by Samsung for $650 million, Swedish biometrics company Fingerprint Cards witnessed its stock skyrocket by 50%. With the recent addition of fingerprint readers in Apple smartphones and the publication of the press release through a publicly traded wire company called Cision, Reuters was quick to cover this acquisition by the Korean phone maker. As Fingerprint Cards debunked the fake news, Cision came under heavy criticism and its stock lost 5% of its value before the end of the day.

SPENCER PHARMACEUTICAL

Spencer Pharmaceutical was the target of a similar pump and dump scheme, as its CEO and Canadian fraudster Jean-François Amyot used PR agencies under his control to spread bombastic fake news on the Boston-based research company. The agencies reported Spencer Pharmaceutical received a $245 million unsolicited takeover bid from the Al-Dorra group, a Middle Eastern company. Amyot was sentenced by a Massachusetts court to pay $7 million to harmed investors.

ANZ

Australian Whitehaven Coal got hit by shocking news. The Australian and New Zealand Banking group (ANZ) had just announced the withdrawal of no less than $1.2 billion in funding for their mining project with ANZ. The statement made the headlines of several Oceanian media outlets and Whitehaven Coal's market value experienced a $314 million drop. Soon after the beginning of the Australian financial regulator investigation, Jonathan Moylan, a 25-year-old activist from Newcastle pled guilty to disseminating false information about the bank and coal mining figure, achieving international coverage for the controversial mining project.

2012

BANK OF AMERICA

A Bank of America CEO letter, seemingly signed by Brian Moynihan, started off with an explosive statement: "Today, it's time to acknowledge that our Bank isn't working anymore—not just for the market, but for people, our real customers..." The letter was, of course, the work of an activist group, rallying under the "Your Bank of America" banner, to raise awareness on the lack of significant change in the governance and practices of the institution during and after the 2008 financial crisis. After the Dow Jones was duped BOA's stock fell 3%.

GOOGLE / ICOA

Google is well known for its tech company acquisitions. When a spoofed press release from mid-sized Wi-Fi hotspot company ICOA posted on PRNews.com touting its acquisition by Google, it came as a believable surprise to some specialized news outlets such as TechCrunch, as well as to many investors. ICOA, a penny stock traded on speculative market OTC Pink, peaked at more than five times its original value, before the SEC halted trading.

2012

SHELL

Shell was targeted by a group of environmental activists. A spoofed website displayed on its homepage a video showing a lady being splashed by an oil-pump-shaped fountain, during a party celebrating the launch of new drilling operation off the Alaskan. The video and the website alongside with a press release used to share them were all fake and part of an operation to raise awareness.

2011

GENERAL ELECTRIC

After revelations of The New York Times detailing how General Electric did not pay any tax during the previous year, the American conglomerate was struck by a hoax. A fake press release, posted on a spoofed website, announced GE would donate back to the government the entirety of their $3.2 billion tax refund. The fake news was picked up by the Associated Press, which posted the information on its wire service. Before the AP sent out a retraction 35 minutes later, GE stock was down half a point. The activist group The YesMen claimed the hack.

2010

CHEVRON

Amazon Watch, RAN and The YesMen teamed up to hack Chevron's corporate communication. Those three activist groups created a fake website and sent it to many media organizations with a fake press release titled "Oil Companies Should Clean Up Their Messes, we agree!" The quotes falsely attributed to Chevron's VP for Policy, Government, and Public Affairs and its Chief Creative Officer, deceived a few media outlets such as Fast Company.

GENERAL MILLS

General Mills was the victim of an obvious hoax. A press release claimed President Obama had ordered a full investigation of the company and cited several fictitious recalls. It was shared by several major news outlets, such as Wall Street Journal Online, Reuters, Fox Business News and Dow Jones Newswire. The release, which was not followed by market backlash since it was published around midnight, used a New York dateline while General Mills is based in Minneapolis, misspelled "yoghurt," and indicated "Steve Sanger," the company CEO, as a contact person, with a phone number located in New Zealand. Fooled journalists blamed PRNewswire, whose services are used by some of its brands, though not General Mills, for publishing the release in the first place.

KOCH INDUSTRIES

Koch Industries, one of America's largest privately held companies, released a short announcement where the group appeared to cease all funding for climate change. This sudden twist in the industrial group communication was nothing but a masquerade. The press release and the fake website were created by an anonymous group of activists calling themselves "Youth for Climate Truth."

8 TAKEAWAYS FOR PR OFFICERS, DECISION MAKERS AND JOURNALISTS

The analysis of the selected cases, whether they have been orchestrated by fraudsters or activists, reveals a few insightful trends.

1. In all cases, journalists published the information with insufficient fact checking, lacking the time or the means to do it properly. When they tried to verify the authenticity of the fake material with a routine check on the linked newsroom or quick call to the contact number, they were tricked by the fake website or fake press relations services set up by the attacker.

2. When a business wire, news agency or a journalist shares the information, it validates and grants the fake information with new levels of legitimacy and credibility. Readers and even other press and media will be much less likely to check it. The journalist or the agency that shares the fake information because of insufficient verification takes the responsibility, especially if that journalist or agency is the first to break the news.

3. Content crafted by fraudsters is false yet always plausible, even in the most far-fetched hoaxes.

4. Hackers' favorite medium is, by far, the press release, whose traditional format is easy to efficiently spoof at roughly no cost.

5. The channels used to spread misinformation are generally multi-tiered: fake emails, fake newsrooms or websites, fake phone numbers... This combination of various levels engineered to give the appearance of truth makes the traditional verification work useless if the person who undertakes it does not personally know the author of the information.

6. Business and official wires do not prevent corporate communication hacking. Their lack of scrutiny even tends to amplify the effect of a hoax that makes it through their verification process, lending it a lot more credibility for a journalist or an investor.

7. Even the most secure systems, such as the SEC databases, can be manipulated.

HOW CAN COMPANIES PROTECT THEMSELVES?

Ensuring the security of corporate information is essential to safeguarding a company's image and interests. To do so, a journalist must be able to quickly and easily check the source and integrity of any communication material. The success of this verification process thus depends both on the good practices of media professionals and on the company's ability to properly certify its contents, then to make this certification accessible with as little time and effort as possible.

As the preliminary step before verification, the certification process must be permanent, impossible to spoof or falsify while staying accessible for the verifying party. Furthermore, to keep control of the time of publication and avoid official information leaks, the certification process must keep the content of document secret and only confirm the integrity and source of a document submitted by the verifier. Finally, it is essential to clearly separate the verification process from the document itself, since a fake document can link to a fake verification interface the same way it can refer to a fake PR team contact number.

Wiztrust allows companies to realize such a certification process in a couple seconds, harnessing the blockchain's distributed ledger immutability and cryptographic security features. With just two clicks, any corporate communication team can anchor the digital signature of a press release, a picture or a video, on Wiztrust.com. A journalist can then verify that the content they receive and are about to publish is legitimate and authentic with the same efficiency. For media and corporations, blockchain-based certification is the most trustworthy process to prevent corporate information hacking.

Multi-channel communication is also a great complement to certification for a company willing to mitigate the risks. It is far more difficult for a hacker to spoof convincingly or to gain access to 8 or 10 communication streams (email, newsroom, website, wire, social media...) with secure authentication, rather than just a couple of them. A company that uses a communication platform such as Wiztopic to broadcast regularly and simultaneously its official information through many different channels is already making a potential fraudster's or prankster's life much more difficult.

As communication evolves with emerging technologies, trust in corporate and financial information is becoming the number one priority for journalists, analysts and investors. Financial institutions and public companies, especially their communication and PR leaders, must innovate to match these new expectations and secure their reputation and financial stability.

DISCLAIMER

Wiztrust is developed by Wiztopic, a software publisher of the first fully compliant platform to help financial institutions and publicly traded companies manage their official communication. Wiztopic users can easily manage content, publish them across all their communication channels and track their performance, in a simple and secure interface.

CONTACT :

Matthew Kaiser

matthew.kaiser@wiztopic.com

(w) 646 - 880 - 9694

FOLLOW US !

wiztrust

Certified with wiztrust