



Check Point®
SOFTWARE TECHNOLOGIES LTD

The history, evolution and future of social engineering



SECURE YOUR EVERYTHING™

According to Wikipedia, social engineering is the psychological manipulation of people into performing actions or divulging confidential information. To put it in simple words – making people believe something and act upon it.

Social engineering techniques vary, however all of them are designed to take advantage of human nature and emotions, to achieve the attacker's goal. Inherent human traits that social engineers take advantage of is wanting to belong, be accepted and follow social norms. While there are different methods to social engineering attacks through different channels, the overall approach is the same.

So how did this all begin?



The history and evolution of social engineering

The first recorded social engineering

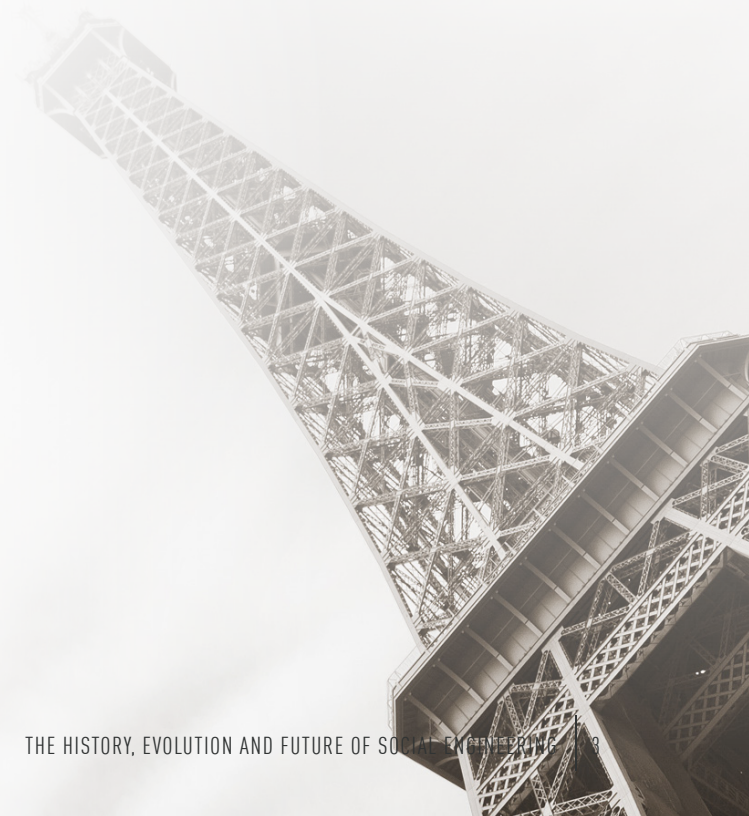
Arguably the earliest social engineering attack was performed by the snake in the Adam and Eve story in the book of Genesis. The snake, which represents a form of the devil, convinced Eve to take a bite from the forbidden fruit in the claim that God was saving the special powers these apples hold to himself. The snake was playing to Eve's greed, and gained her trust through a social engineering tactic called trust/distrust – make a person distrust someone else and thus appear to be on their side, and gain their trust in you.

Jumping ahead to more recent times - in the 20th century there were numerous crazy and very original social engineering scams. Here are a couple of them:

The Eiffel Tower Sale

In 1925, Victor Lustig, a charming con artist, settled in Paris. He then came up with a crazy yet brilliant scam – selling the Eiffel tower for scraps. In those years the Eiffel tower's fame was declining with very few visitors and strong criticism. The financial difficulties of maintaining the structure created a noise around the possible idea of selling the monument.

Victor Lustig saw this as a golden opportunity for a scam like nothing before. He managed to fake a letterhead from the city of Paris claiming he has the right to sell the tower, as well as an access card to the Eiffel tower. He then tracked down the most prominent scrap dealers in the city and invited them to a “secret meeting” at the Crillon hotel.



Five dealers answered the invitation, and Victor presented them with the opportunity: the city needs to get rid of the expensive to maintain monument, and the highest bidder will get ownership over the entire tower's materials. He then took the men to visit the tower with his fake access card, making him more credible in their eyes.

The bids started flowing in and one young dealer, whom Victor had his eyes on especially for his lack of experience, bought in to the scam and purchased the tower from Victor. When he came to the tower and claimed ownership to the baffled guards, Lustig had already fled the country. The victim was so ashamed that he never submitted a claim against Lustig.

It is said that Victor actually managed to pull off this scam more than once.

The \$10 Million phone call

Can you steal over \$10M dollars over the phone? This is the unbelievable story of Stanley Mark Rifkin, a computer-repair consultant in the 1970s. Rifkin worked for a 3rd party contractor of the Security Pacific National Bank wire room, and his job was to back up the computers in the wire room in case of a shut down.



Through his daily job, Rifkin learned all about the procedures of wiring money in the bank. He understood that there is a daily code that the clerks in the wire room use to approve money transfers. Since the clerks didn't want to memorize the code every day, they wrote it down on a note and put it somewhere so they can quickly find it when needed.

One day Rifkin went into the wire room for his daily job, and took notes of the wiring procedures, as well as memorized the daily code. He then went to a pay phone in the same building's lobby and called the wire transfer room he was just in. He impersonated as a member of the bank's international department, and through the regular wiring procedures he had spent his time learning on his daily job, he managed to fool the operator into transferring over \$10 Million dollars to a Swiss bank account he had previously opened for this scam.

A few days after the phone call Rifkin flew to Switzerland, picked up his cash, and gave \$8 million to a Russian agency for a pile of diamonds.

Fun and weird fact – this amazing scam eventually made it into the pages of the Guinness Book of World Records in the category of “biggest computer fraud”, although no computer had been used to pull off this scam.



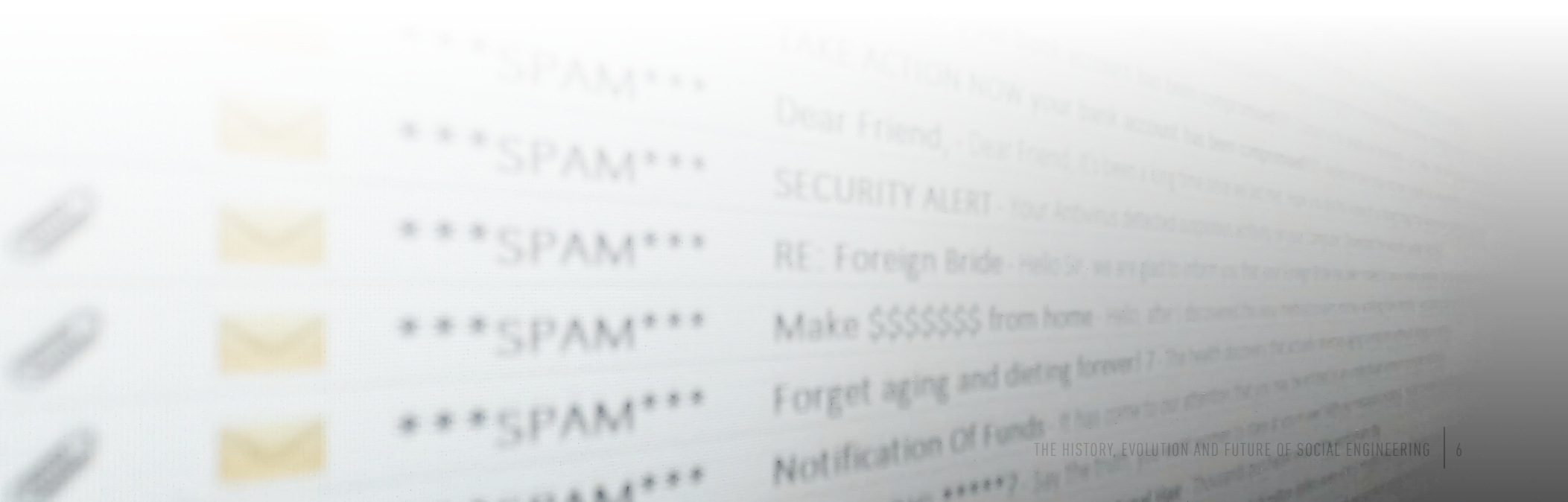
The Nigerian prince

This brings us to the later and more familiar form of social engineering – email scams. Let's be honest, no social engineering story is complete without the infamous Nigerian Prince scam.

The Nigerian prince (also known as the 419 scam), is perhaps the longest lasting email phishing scam to date. The Nigerian Prince scam is an advance-fee scam. The scam typically involves promising the victim a significant share of a large sum of money, in return for a small up-front payment, which the cyber criminals claim will be used to get that promised large sum of money.

If a victim makes the payment, the criminal either invents a series of further fees for the victim to pay or simply disappears.

The Nigerian Prince scam has been executed through fax and traditional mail, and then evolved into online communications like emails. It is a classic quid pro quo scam which means something for something – offering a victim a reward in exchange for a desired action.



Email Social Engineering

Social engineering through emails started in the 1990's, when electronic mails (emails) started to be widely used by the public. With the increased daily use of emails – in 1996 attackers launched an attack on AOL users, sending them messages while posing as AOL employees through the AOL instant messenger and email systems. Those messages would request users to verify their accounts or to confirm their billing information, which cybercriminals would then steal.

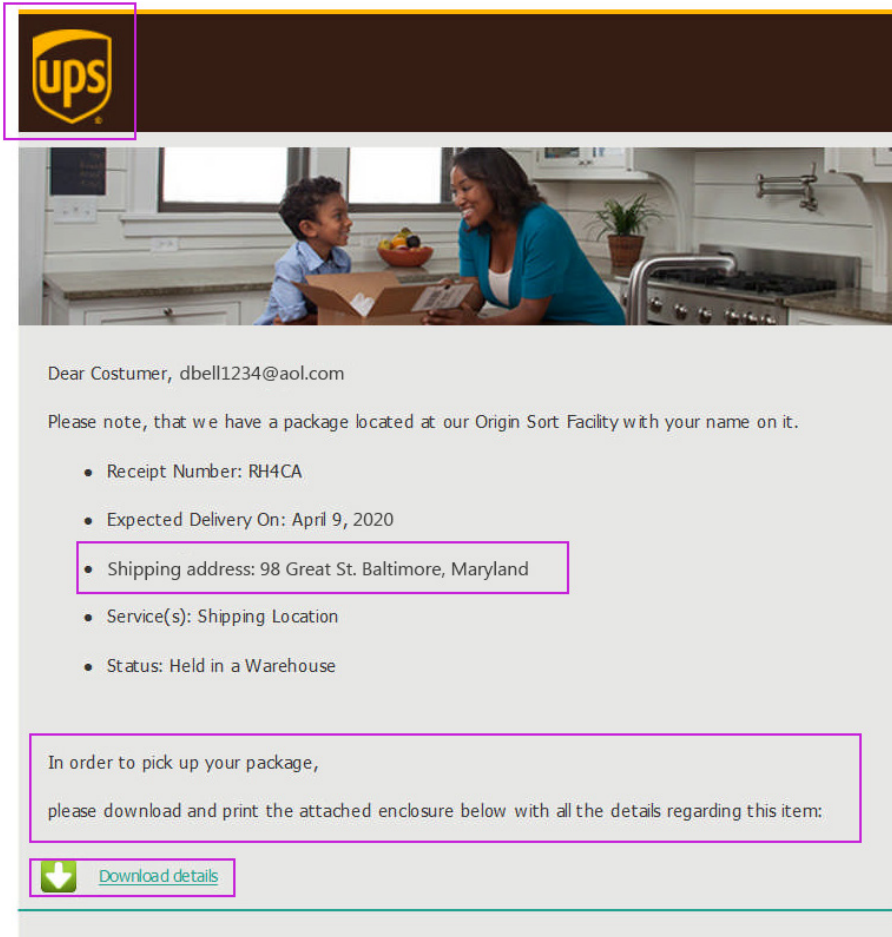
Although it sounds basic now, this attack was pretty successful simply because nothing like it had ever been done before. With the rise of online payment platforms and eCommerce sites like PayPal and eBay, came the exploitation of these platforms to scam users. In late 2003, attackers registered dozens of domains that impersonated as the platforms. They used email worm programs to send out spoofed emails to PayPal customers which led to spoofed sites that asked victims to update their credit card details and other identifying information, which the attackers then stole.

In late 2008, Bitcoin and other cryptocurrencies are launched. This allows transactions using malicious software to be secure and anonymous, changing the game for cybercriminals. In September of 2013, Cryptolocker ransomware infected 250,000 personal computers, making it the first cryptographic malware spread by downloads from a compromised website.

Today, the most common email attacks are Spear Phishing, Business Email Compromise and Malware.

Spear Phishing

Spear Phishing attacks are specifically targeted at a particular individual or small group. In this case, an impersonation email from “UPS” looks extra convincing thanks to proper graphic elements such as the logo, image and the fonts.



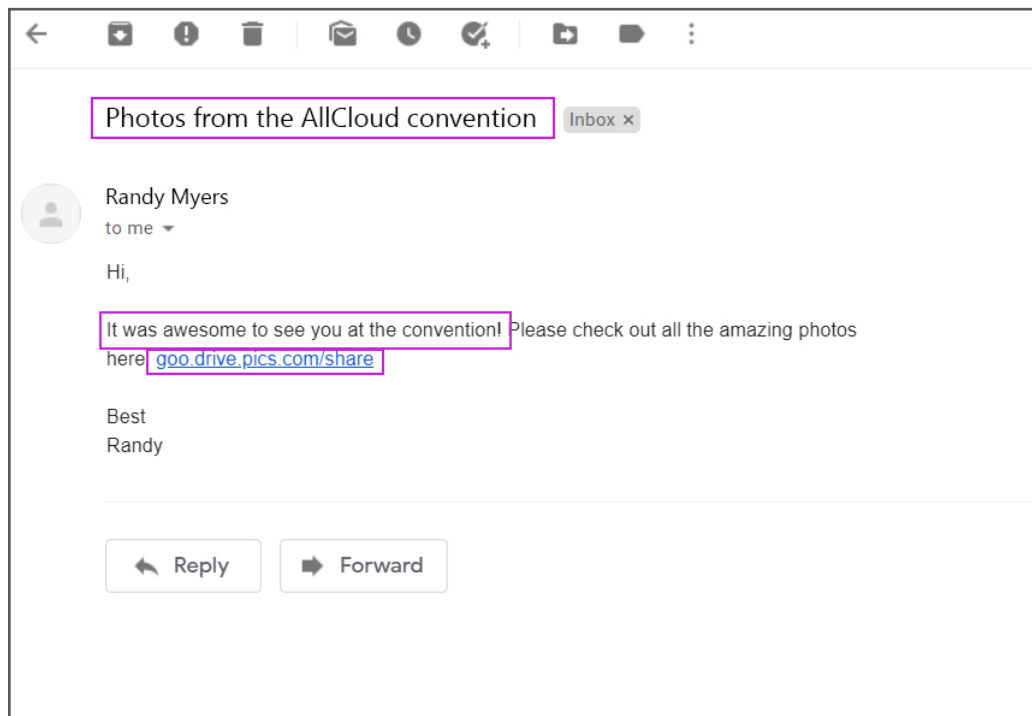
What’s more, through collecting available online information on the victim, the attacker is able to know the victim’s full address.

Through using it in their fake email from UPS regarding their so-called package needing to be delivered, the attackers increase the likelihood of the victim clicking that “download details” button, which will download a malware to their device.

Malware

Continuing with the targeted attacks, how easy is it for someone to know you've attended an event or a conference? Pandemic life aside, we've all been to many conferences that our entire LinkedIn network knew about.

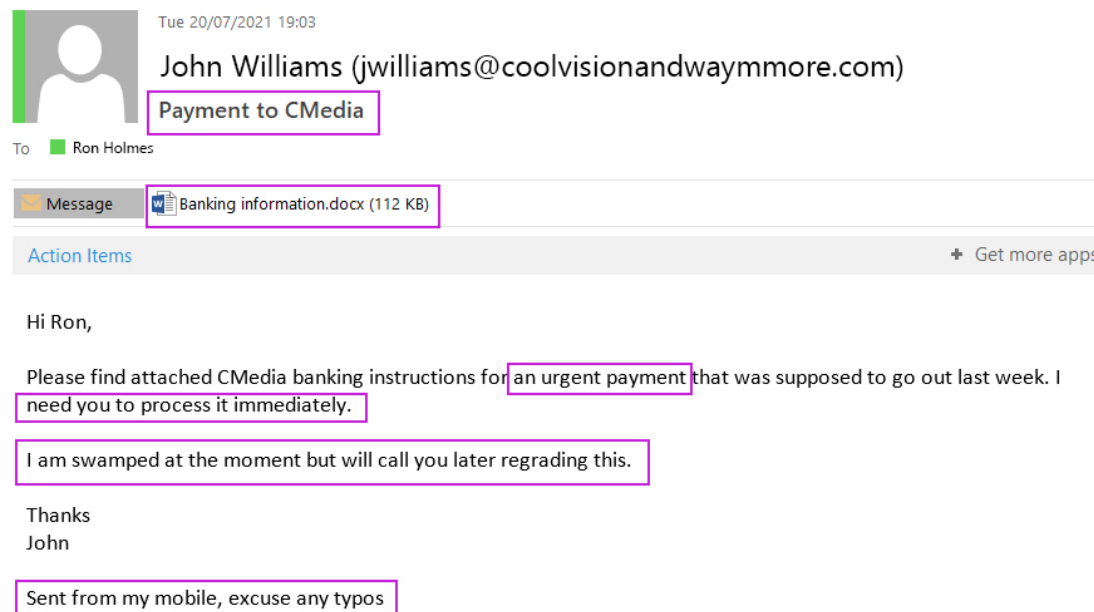
In this case, attackers can pretty easily find the email addresses of everyone that attended a certain convention on LinkedIn, and send them an email with a link to the "photos from the event". This link, once clicked, would download a malware to the victim's device. Pretty easy right?



Business Email Compromise (BEC)

BEC attacks are some of the most costly and devastating attacks. Cyber criminals carry out BEC scams through spoofing email accounts and websites, use recon to send spear-phishing emails, and sometimes use malware.

Here is an example of an employee getting an email from his manager to immediately transfer money to a vendor, with the vendor's details. This email could look very legit to the unsuspecting employee looking to do their job right, and could (and a lot of the times does) result in a successful money transfer.



The Possible Future of Social Engineering in Emails

Data Breaches Lead to More Scams

Besides super targeted attacks, cyber criminals can cast a wide net and send out mass emails to victims of a data breach, leveraging their leaked information to divulge them into doing whatever it is they want them to do.

A real recent example is a sextortion campaign. Attackers got access to users' LinkedIn account credentials through a data breach, and mass emailed those users saying that they had hacked their camera, and this is their cameras password: (the LinkedIn password). Since so many people use the same password for different things, a lot of the victims actually fell for this scam when the attackers threatened to share private videos of them if they don't do as they say.

With the state of cybercrime, data breaches are bound to keep happening on larger scales, and these follow-up attacks will continue to happen in greater numbers.

From: Save Yourself
Subject: I recorded you - [REDACTED]

Hi, I know one of your passwords is: [REDACTED]

Your computer was infected with my private malware, your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".

My malware gave me full access to all your accounts (see password above), full control over your computer and it also was possible to spy on you over your webcam.

I collected all your private data a [RECORDED YOU (through your webcam) SATISFYING YOURSELF!]

After that I removed my malware to not leave any traces and this email(s) was sent from some hacked server.

I can publish the video of you and all your private data on the whole web, [REDACTED] of all contacts.

But you can stop me and only I can help you out in this situation.

The only way to stop me, is to pay exactly 800\$ in bitcoin (BTC).

It's a very good offer, compared to all that horrible shit that will happen if I publish everything!

You can easily buy bitcoin here: www.paxful.com , www.coingate.com , www.coinbase.com , or check for bitcoin ATM near you, or Google for other exchanger.

You can send the bitcoin directly to my wallet, or create your own wallet first here: www.login.blockchain.com/en/#/signup/ , then receive and send to mine.

My bitcoin wallet is: 1Eim8U3kPgkTRNSFKN49jgz9Wv4A1qmcjR

Copy and paste my wallet, it's (cAsE-sEnSEtiVE)

I give you 3 days time to pay.

As I got access to this email account, I will know if this email has already been read.

If you get this email multiple times, it's to make sure that you read it, my mailer script is configured like this and after payment

Recon Has Never Been Easier

The most important stage in a targeted social engineering attack is the recon stage, when attackers collect as much information on their target as they possibly can.

In 2021, collecting information on people is easier than ever. In fact, attackers don't even need to work very hard – we willingly give them all the information they need through social media.

Just based on a worker's social media account, whether it is Instagram for their personal life or LinkedIn for their professional life, and combining all this information with information that can easily be found through a simple google search, one can easily create an extensive profile of their victim. This profile may include events they attended, restaurants they like, coworkers they interact with the most, if they are looking for a new job, who is their direct manager and so on.

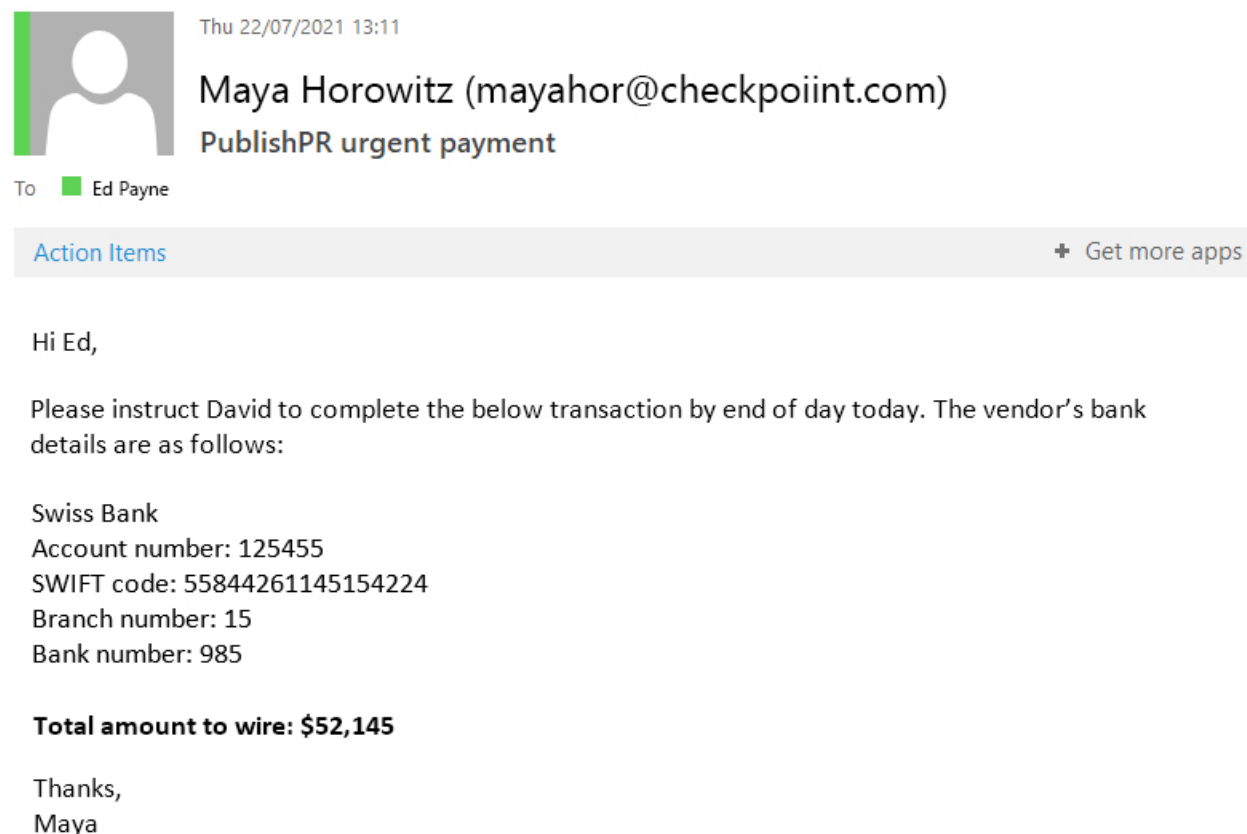
Just like the attacks we explored earlier, the more we share on social media, the easier it is for attackers to target us and our employees.



Deep Fakes Are On the Rise

Deep Fakes may seem like buzz words at the moment, but the technology is likely going to be prominent in attacks in the very near future.

In the example below there's a BEC email like we showed earlier in this article, where a senior management employee asks their



The screenshot shows an email interface. At the top left is a grey profile icon with a white circle. To its right is the text 'Thu 22/07/2021 13:11'. Below the icon is the name 'Maya Horowitz (mayahor@checkpoint.com)' and the subject 'PublishPR urgent payment'. Below the subject is the recipient 'To Ed Payne'. A grey bar contains 'Action Items' on the left and '+ Get more apps' on the right. The email body starts with 'Hi Ed,' followed by a request to instruct David to complete a transaction by end of day today, with bank details for a Swiss Bank. The total amount to wire is \$52,145. The email ends with 'Thanks, Maya'.

Thu 22/07/2021 13:11

Maya Horowitz (mayahor@checkpoint.com)
PublishPR urgent payment

To Ed Payne

Action Items + Get more apps

Hi Ed,

Please instruct David to complete the below transaction by end of day today. The vendor's bank details are as follows:

Swiss Bank
Account number: 125455
SWIFT code: 55844261145154224
Branch number: 15
Bank number: 985

Total amount to wire: \$52,145

Thanks,
Maya

subordinate to transfer money to a vendor immediately. An email might not be enough in case of a very savvy employee. But what if they then get a phone call from that same manager?

In this case, [we've deep faked Maya Horowitz](#), our VP Research's voice, telling an employee to complete the wire request mentioned in the email they had received. All it took is opening a \$30 account on a platform that creates deep fake voices out of samples provided.

As this technology progresses, it will be widely available and harder to tell the real from the fake, making attacks even harder to prevent.

How to Stay Safe

Staying safe from email attacks requires a two-fold strategy. The first layer is making sure your employees and users possess healthy security awareness skills.

Some practical tips for users include:

- Always look with a critical eye on emails containing links and files
- Never fill in your account credentials or any sensitive information when reaching a webpage through a link in an email
- Be cautious when getting an email with a sense of urgency
- Double check the source and credibility of emails with any kind of financial requests

The second layer has to be a solid security solution that prevents these scams from ever reaching the users in the first place.

Check Point's [Harmony Email & Office](#) is a complete solution for email and collaboration apps security. The solution prevents phishing and malware in emails with 99.8% block rate, so attacks are prevented before they happen. Start a free trial [here](#).

