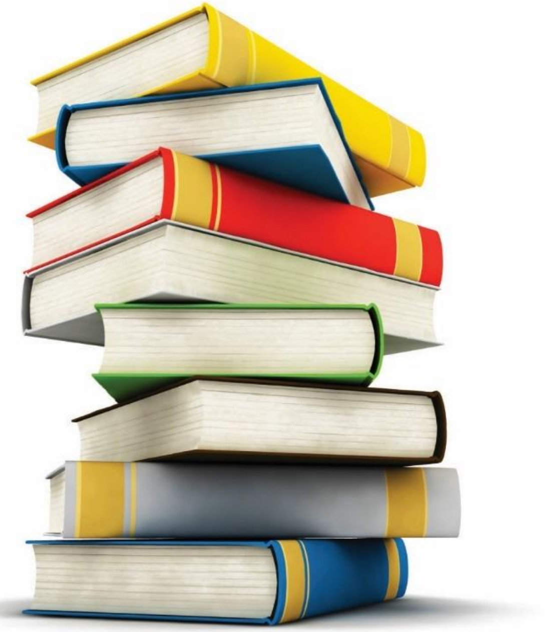
TECHNION
Israel Institute
of Technology

Table of Content

Anyone can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis.
Bruce Schneier



1 | December | 2022

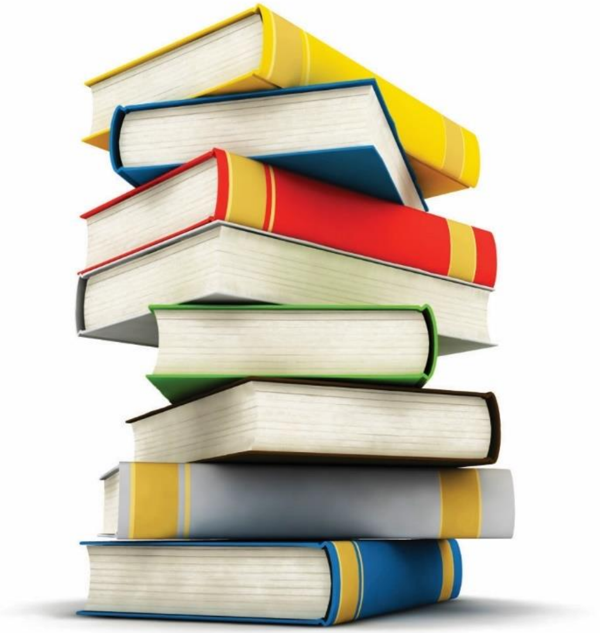
1. A sophisticated scammer group has stolen at least €480 million from victims in France, Belgium, and Luxembourg since 2018, according to researchers at Group-IB. The gang uses a highly detailed scam kit called "CryptosLabs," which impersonates investment portals from more than forty major European financial entities.

Right out of the block, the victims are promised high returns on their capital. To find the 'investors', scammers leave messages on the dedicated investment forums or use legitimate advertising mechanisms on social media and search engines to promote the scheme. To appear trustworthy, such ads feature logos of notable banking, fin-tech, crypto, and asset management companies active in France, Belgium, and Luxembourg.

To read the complete article

What did we learn? If it is too good to be true, it is probably not true. Do your due diligence thoroughly and carefully.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them



2. Cyber skills fund military efforts

1 | December | 2022

South Korea's intelligence services, national police, and five ministries published a warning about the North's (DPRK) tactics that opens as follows:

DPRK IT workers are located all around the world, obfuscating their nationality and identities. They earn hundreds of millions of dollars a year by engaging in a wide range of IT development work, including freelance work platforms (websites/applications) and cryptocurrency development.

Those workers' real job, the warning asserts, is "earning foreign currency and financing nuclear and missile programs for the regime."

To read the complete article

What did we learn? Check carefully who you hire and pay. You might be helping the bad guys funding their military efforts.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

3. The history of Phishing from 1996 till 2022

1 | December | 2022

The term “phishing” was coined back in 1996, when cybercriminals attacked users of America Online (AOL), the largest internet provider at that time. Posing as AOL employees, the scammers sent messages asking users to verify their accounts or asking for payment details. This method of phishing for personal data is still in use today, because, unfortunately, it continues to yield results.

Also in the 1990s, the first online scams appeared. When banks began to roll out internet banking, scammers sent text messages to users supposedly from relatives with an urgent request to transfer money to the details given in the message.

By the early 2000s, charity had become a common scam topic: for example, after the massive Indian Ocean earthquake and tsunami of 2004, users received messages from fake charities pleading for donations. At around the same time, phishers started targeting online payment systems and internet banks. Since user accounts in those days were protected only by a password☹, it was enough for attackers to phish out this information to gain access to victims’ money. To do this, they sent e-mails in the name of companies such as PayPal, asking users to go to a fake site displaying the corporate logo and enter their credentials. To make their sites look more credible, cybercriminals registered multiple domains all very similar to the original, differing by just two or three letters. An inattentive user could easily mistake a fake for a genuine bank or payment system website. In addition, scammers often used personal information from victims’ own social media pages to make their attacks more targeted, and thus more successful.

As time progressed, online fraud became ever more sophisticated and persuasive. Cybercriminals learned how to successfully mimic the official websites of brands, making them almost indistinguishable from the original, and to find new ways to approach victims. There appeared services specializing in creating fake content, at which point phishing really took off. Now not only the personal data and finances of ordinary users were in the firing line, but politicians and big business as well.

This report examines the main phishing trends, methods, and techniques that are live in 2022."

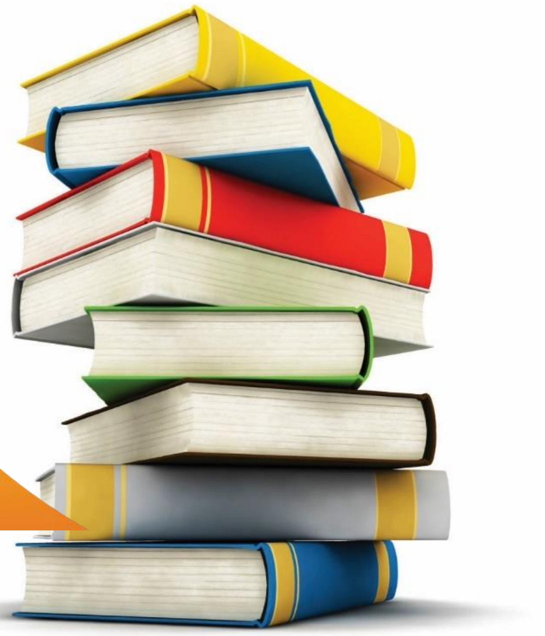
To read the complete article

What did we learn? The complete article is very interesting with examples in different languages and will help you to strengthen your awareness.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you’ve got – Don’t give it to them

TECHNION
Israel Institute
of Technology

4. Who is more vulnerable to phishing?
Younger or older?
Male or female?



1 | December | 2022

Digital natives aged between 18-39 are the most vulnerable age group for phishing scams, according to new data from security awareness training company SoSafe.

It finds that 18-39 year-olds have an average click rate of 29 percent on phishing emails, which drops to 19 percent among older age groups.

The report also shows men tend to click on phishing links more often than women. 23 percent of male participants opened at least one of the simulated phishing emails, with the average click rate among female participants more than 10 percent lower.

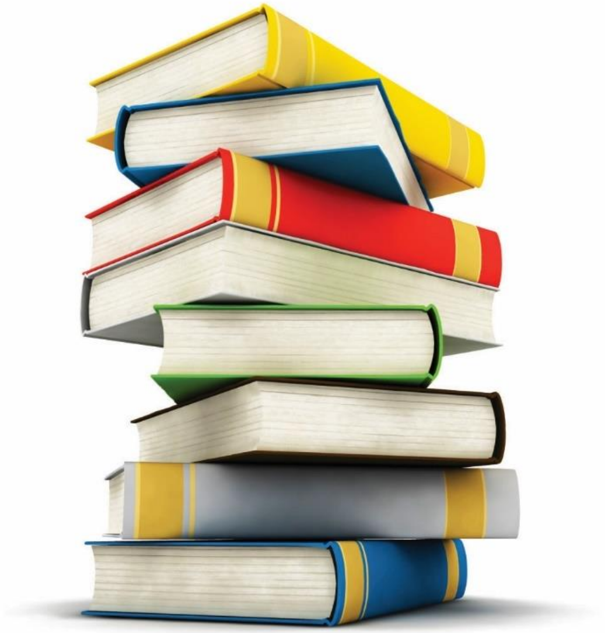
Public sector organizations are most vulnerable to phishing attacks (with an average click rate of 36 percent) while staff in manufacturing companies are least likely to click on harmful emails (19 percent).

To read the complete article

What did we learn? We are all vulnerable. Some more and some even more. Young male in public sector is most vulnerable. ☺

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

5. Beware if you harass people, it might be Double-edged sword

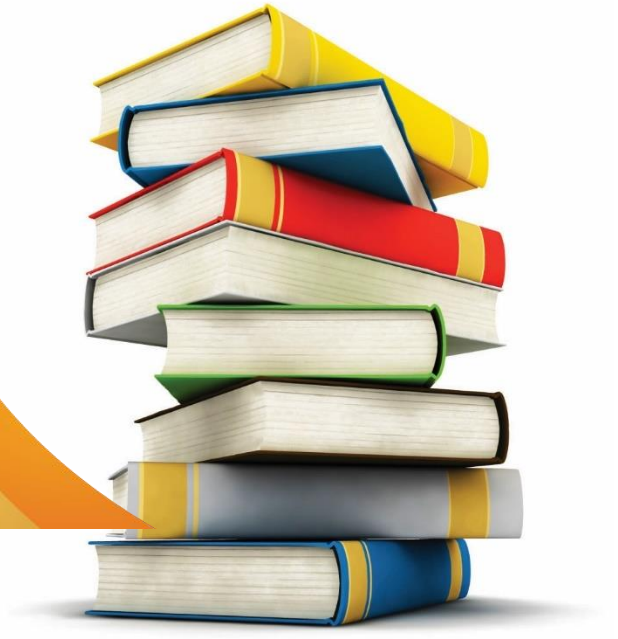


Many people suffered terrifying cases of harassment. It may include numerous threatening text messages, countless emails, and physical package deliveries. It understandably has bothered them to not know the identity of their adversary. In this case, they know, and here are details about the investigation. A website called "Get Revenge On Your Ex" (https://www.getrevengeonyourex.com) has been around for over a decade. It is one of many services which will blast text messages and emails to any victim for a small fee. In September 2022, the site was breached and all user data was stolen. While most breaches include damaging details which could harm innocent victims. In this case we encounter a breach which shares the exposure of criminals who think they are anonymous. I believe this is the kind of success should be discussed when the ethics of data access are debated.

To read the complete article.

What did we learn? Oh, those who use PayPal or even Crypto to pay for such services, are extremely exposed. Once online investigation starts digging into such data, they may be the one who feel harassed.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them



6. A question from the previous newsletter:

What is the best defense against ransomware?
A. Purchase comprehensive cybersecurity insurance.
B. Back up your data regularly.
C. Regularly update all your devices and software with the latest security patches.
D. Use a good Antivirus tool.

The correct answer is -B. If your data is encrypted, backup is your saver.
A,C and D are good and important but definitely not sufficient.
A will give you money but not your lost data.
C and D can’t guarantee a breach won’t happen.

New Question

You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should: (mark all correct answers)

- **A. Reply to the text to confirm that you really need to renew your password.**
- **B. Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.**
- **C. Click on the link. If it takes you to the vendor’s website, then you’ll know it’s not a scam.**
- **D. Login to vendors website via a link you know to be correct and take it from there.**

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you’ve got – Don’t give it to them