TECHNION
Israel Institute of Technology

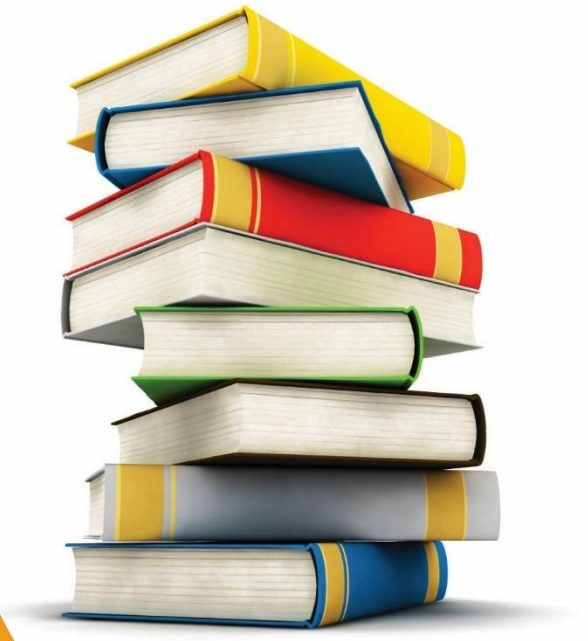


Table of Content

"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture." — Britney Hommertzheim

1 | July | 2022

1. For months now, millions of Facebook users have been duped by the same phishing scam that cons users into handing over their account credentials.

According to a report outlining the phishing campaign, the scam is still active and continues to push victims to a fake Facebook login page where victims are enticed to submit their Facebook credentials. Unconfirmed estimates suggest nearly 10 million users fell prey to the scam, earning a single perpetrator behind the phishing ploy a huge payday.

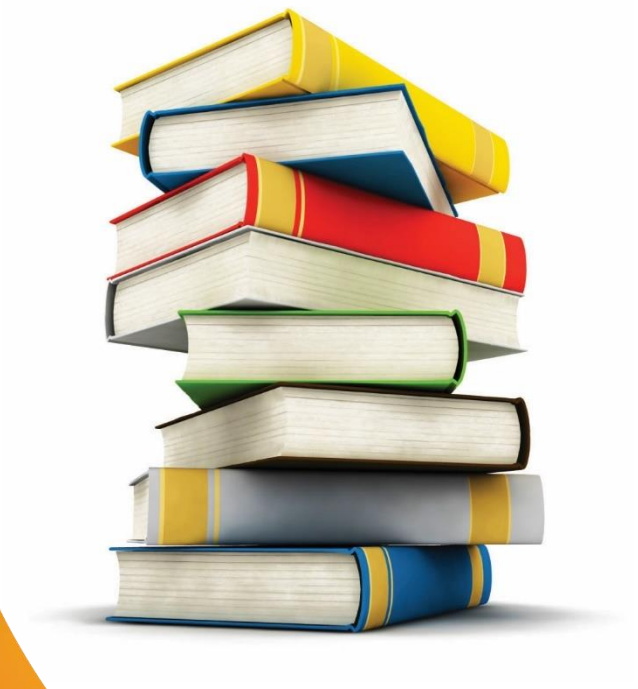
According to a report published, the phishing campaign began last year and ramped up in September. Researchers believe millions of Facebook users were exposed each month by the scam. Researchers assert that the campaign remains active.
The crux of the phishing campaign centers around a fake Facebook login page. It might not look immediately suspicious, as it copies Facebook's user interface closely. The threat actor would login to that account and send out the link to the user's Friends via Facebook Messenger. Any Friends that click the link are brought to the fake login page. If they fall for it the credential-stealing message is forwarded to their Friends. Victims are redirected to pages with advertisements. Each of these pages generates referral revenue for the attacker, researchers said.

To read the complete article

What did we learn? Double check the authenticity of the site you visit. By falling you may fail your friends. Even giants like Facebook might fail in detecting an attack.

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



2.Romance scams

1 | July | 2022

"If you were one of the millions of people who watched Netflix's The Tinder Swindler, you may have shaken your head in wonder at how women could be allegedly hoodwinked out of millions of dollars.

They should have known better, some say. In reality, it's not that simple.

People fall for these scams for the same reasons that they fall prey to cold-call scam texts claiming that their loved one is in hospital and fees urgently need to be paid: When emotions are involved, rational thinking can go out of the window."

To read the complete article

"An Abbotsford woman is warning others about a "romance scam" that recently resulted in her elderly mom losing $270,000.

"Sandra," who did not want her real name used, said her mom, "Rita," cleared out her registered retirement savings plan (RRSP) and was ready to take out a loan on her home before her family discovered what was happening.

The matter has been reported to the Abbotsford Police Department (APD), but investigating officer Det. Daryl Young with the major crime unit said it's too late for Rita (not her real name).

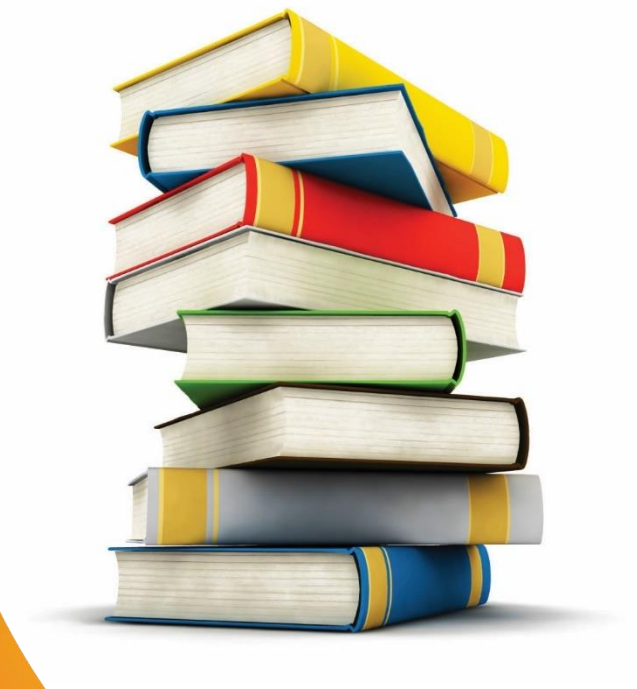
"The sad reality is the money is gone, and so we're trying to take more of an educational stance now – trying to get the word out there that these things are scams," he said."
To read the complete article

What did we learn? When emotions are involved, rational thinking can go out of the window."

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

3. U.S. DoD tricked into paying $23.5 million to phishing actor



1 | July | 2022

Conspirators registered the domain "dia-mil.com", which is very similar to the legitimate "dla.mil, and used it to send phishing emails. These emails were delivered to users of SAM (System for Award Management), which is a vendor database where companies that want to conduct business with the Federal Government register themselves. The phishing messages contained links to a cloned "login.gov" website, where the victimized vendors entered their account details, unknowingly exposing them to attackers. In at least one confirmed case, attackers logged onto one of the stolen accounts belonging to a corporation from Southeast Asia that had 11 active contracts of fuel provision for the United States military at the time. One of them was a $23,453,350 contract with a pending payment for the provision of 10,080,000 gallons of jet fuel to the U.S. DoD. By logging in onto the SAM database as the victimized corporation, attackers changed the registered banking information, replacing the foreign account with one that he controlled.

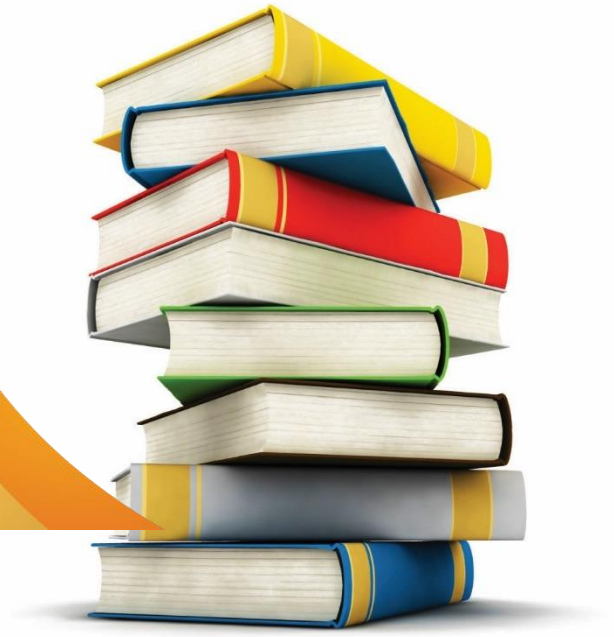
To read the complete article.

What did we learn? One must be very careful and double check the sender's email address. Slight differences make the whole difference. Use bookmarks and not direct/email links as much as possible.

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. Israeli Ministry Illegally Shared Biometric Images of Millions with Unknown Agency



The Population and Immigration Authority illegally shared in the past seven years the facial images of millions of Israelis with an unnamed government agency.
The actions of the Interior Ministry division were disclosed in an official report published last week by Roy Friedman (not our Prof.), the head of the Israel National Cyber Directorate's Identity and Biometric Applications Unit.
Leaky forms are just one more type of data collection to be wary of in an already extremely crowded online field.
To read the complete article

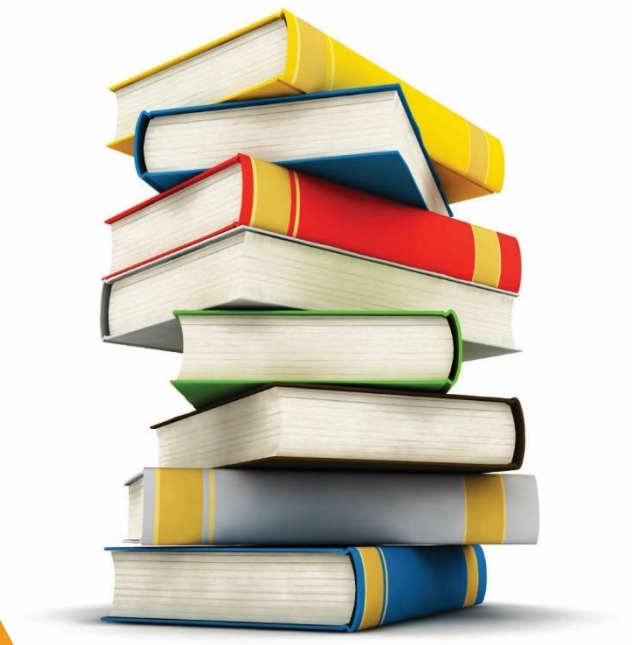
1 | July | 2022

What did we learn? Be very careful sharing data with 3rd parties. Make sure you follow Technion procedures. The regulator may look the other side when Ministry is involved but may be very strict and nagging with others.

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

5. *Home delivery scams*

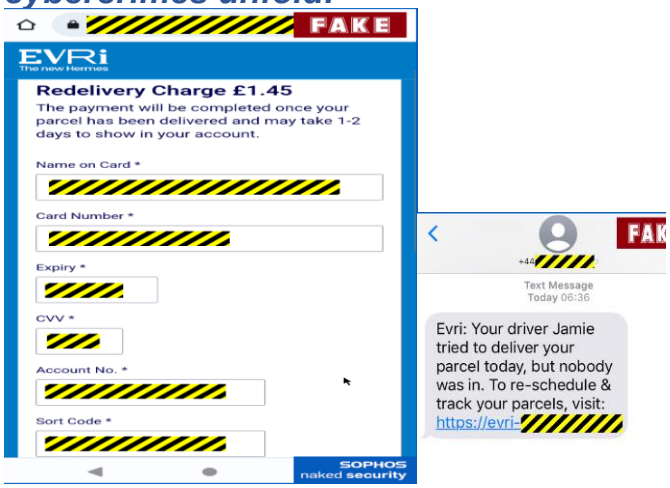


1 | July| 2022

Home delivery scams, where the crooks falsely apologize to you for not delivering your latest parcel, have been around for years.

However, these scams seem to have become steadily more professional-looking during the pandemic, as more and more people have got into the habit of ordering deliveries for everyday shopping instead of heading into stores.

For example, here's a contemporary SMS-based scam (phishing that is kicked off by a text message, or SMS, is wryly known as smishing) that makes a good "picture story" of how these cybercrimes unfold.

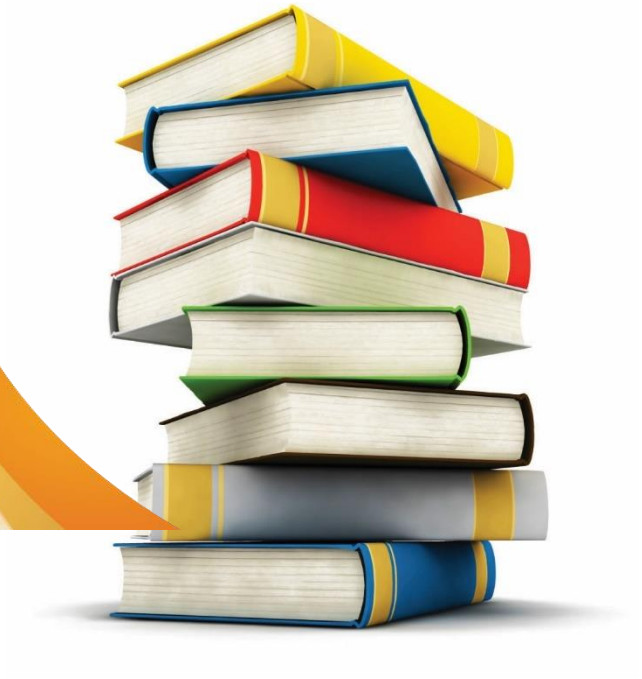


if in doubt, don't give it out.
In this criminal campaign, the scammers were targeting a home delivery company in the UK called Evri."
To read the complete article
What did we learn? Check all URLs carefully (easier on a computer than on smartphone). Steer clear of links in messages or emails if you can. Report compromised cards or online accounts immediately. Check your bank and card statements.

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

6. Q&A



1 | July | 2022

6. Question from the previous newsletter:

When is it ok to reuse a password?

- **A. When you are logging into social media accounts.**
- **B. When it is too hard to remember a long password.**
- **C. Never.**
- **D. When the password is long and complex.**

The correct answer is C. Do not use the same password in different systems. If one of the systems is compromised, this password will let the bad guys login to your other systems.

We are not talking about SSO environment, but completely different and independent systems.

New Question

- **What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?**

1. **That the site has special high definition**
2. **That information entered into the site is encrypted**
3. **That the site is the newest version available**
4. **That the site is not accessible to certain computers**
5. **None of the above**
6. **Not sure**

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