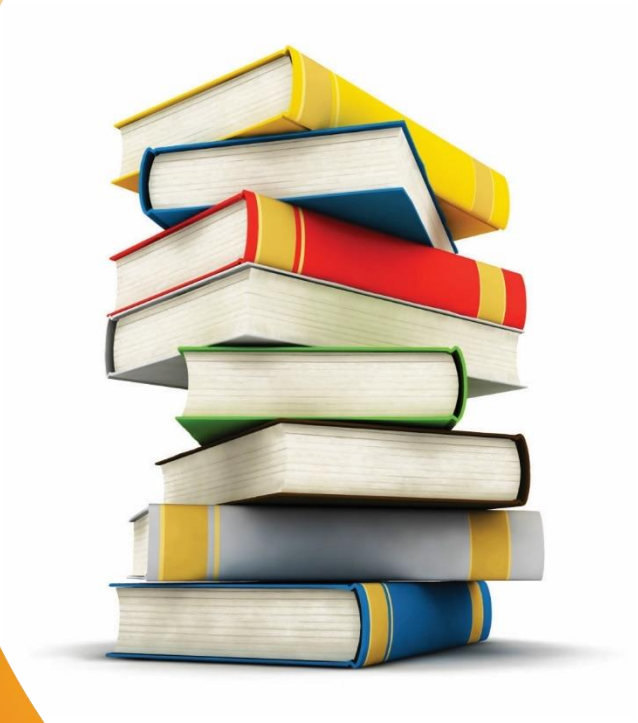
TECHNION
Israel Institute of Technology



1 | June | 2022

Table of Content

Following the phishing awareness email from April Everyone is invited to 60 min training on

June 7th at 10 AM

https://technion.zoom.us/j/4241206358?from=addon

1. "Our 24/7 digital lives mean we're increasingly sitting in front of a screen, whether that's a laptop, a smartphone or another device. That usually means we're also sitting in front of a camera. Some of us rarely used this feature, until the pandemic hit and saw homebound workers and bored students alike switch on their webcams to stay connected with the rest of the world. But while online cameras can provide a lifeline to friends and family, and a near-ubiquitous way of participating in meetings, they also put us at risk.

Whether it's financially motivated cybercriminals, stalkers, bullies, trolls or just plain weirdos, the tools and knowledge to hack webcams have never been easier to find online. That puts the onus on us all to become more aware of the risks and take steps to improve our online privacy and safety. A lot of it is common sense. Some of it needs to be learned behavior.

The truth is that "camfecting" doesn't just invade your privacy. It could seriously impact your mental health and wellbeing. For every creep that's been arrested and jailed, there are many more still stalking the digital world looking for victims."

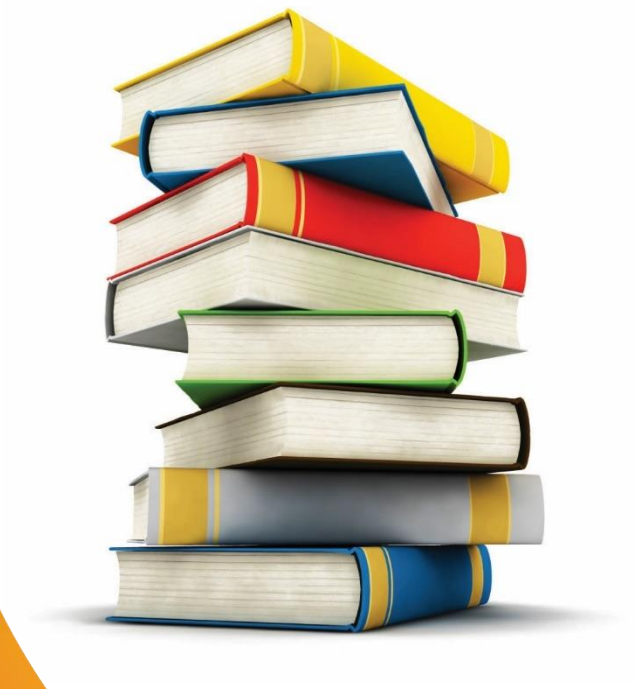
To read the complete article see:

https://www.welivesecurity.com/2022/04/25/webcam-hacking-how-know-someone-spying/

How to prevent webcam hacking: Staying safe from webcam hackers requires alertness and best practice security. Ensure your PC, mobile or smart home device is always on the latest software and pre-loaded with anti-malware software. Make sure it's protected by a strong and unique password or passphrase, as well as two-factor authentication (2FA) if possible. Don't click on links in any unsolicited communications. And cover your camera lens when not in use, although that won't stop criminals from listening in through your microphone.

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.Queen's University, Canada - Life Sciences students facing mass data breach

1 | June | 2022

- Confidential student information in the Life Sciences department was disseminated via email
- The information included student GPAs, student names, student numbers, academic plans, and years of study as of Sept. 2021. Students' sexes and email addresses were also compromised.
- Life Sciences program advisor, said she "inadvertently" attached an Excel class list file containing the compromised information to an email sent out to all fourth-year Life Sciences students. The subject of the email was a networking opportunity.
- Information Technology Services was contacted and has deleted all copies of the email and the attachment in question. The Department quickly notified all students in Life Sciences of the breach and what personal information had been disclosed.
- Queen's apologized to students and is offering support
- To read the **complete article** .

What did we learn?

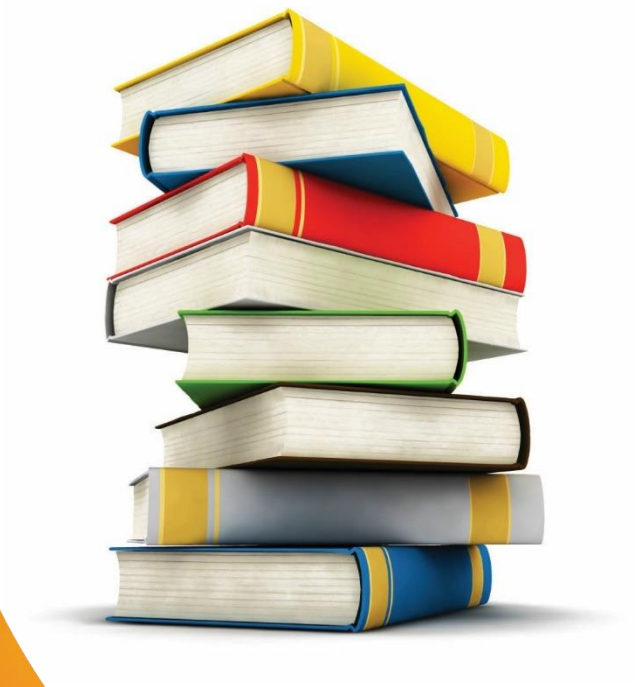
1. The ease of sending an email or sharing a file also brings risks.
2. "inadvertently" mistakes may and will happen.
   a. Try to avoid them, think before you click
   b. If happened, be transparent and ask for immediate mitigation
   c. This is a security incident, act accordingly to **Technion procedure**
   d. Consider adding a password protection to sensitive files.

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. Android malware

These days, the device in your pocket can do far more than call or send text messages. Your smartphone stores almost every aspect of your life, from memories captured as photos to personal notes and schedules, login details and various other kinds of sensitive data.



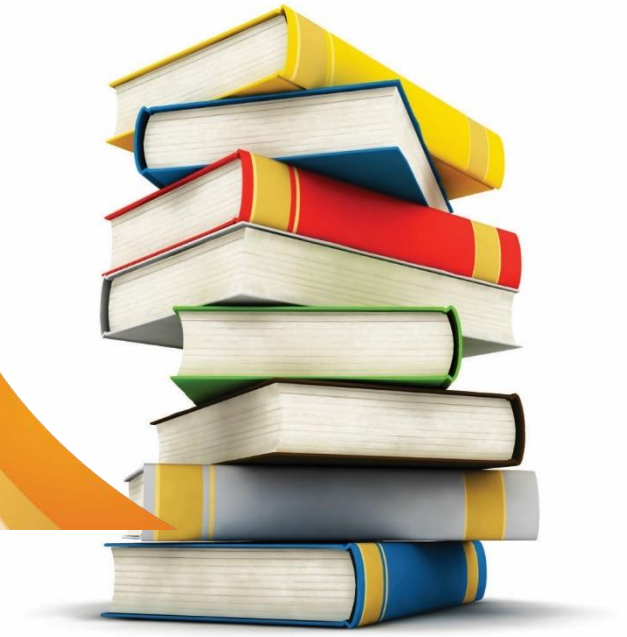
1 | June | 2022

Android-powered devices command more than 70 percent of the mobile operating system market. Add to that the open nature of the Android ecosystem and it's clearer why these devices bear the brunt of malicious attacks on mobile devices and remain a lucrative target for attackers. Google has, of course, introduced a number of privacy- and security-enhancing features for Android devices. Just a few days ago, the company announced that it had stopped 1.2 million policy-violating apps from reaching Google Play last year, among other measures aimed at cracking down on malicious apps. However, this is not to say you should let your guard down when it comes to all sorts of dangers that lurk especially in third-party app stores. To read the complete article.

How to check if your phone (Android or iPhone) has been compromised – Read here

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. Thousands of Popular Websites See What You Type—Before You Hit Submit.

WHEN YOU SIGN up for a newsletter, make a hotel reservation, or check out online, you probably take for granted that if you mistype your email address three times or change your mind and X out of the page, it doesn't matter. Nothing actually happens until you hit the Submit button, right? Well, maybe not

1 | June | 2022

As with so many assumptions about the web, this isn't always the case, according to new research: A surprising number of websites are collecting some or all of your data as you type it into a digital form.
If there's a Submit button on a form, the reasonable expectation is that it does something—that it will submit your data when you click it," says Güneş Acar, a professor and researcher in Radboud University's digital security group and one of the leaders of the study. "We were super surprised by these results. We thought maybe we were going to find a few hundred websites where your email is collected before you submit, but this exceeded our expectations by far.

The behavior is similar to so-called key loggers, which are typically malicious programs that log everything a target types. Meta Pixel and TikTok Pixel, invisible marketing trackers that services embed on their websites to track users across the web and show them ads. For US users, 8,438 sites may have been leaking data to Meta, Facebook's parent company, through pixels, and 7,379 sites may be impacted for EU users. For TikTok Pixel, the group found 154 sites for US users and 147 for EU users. The privacy risks for users are that they will be tracked even more efficiently; they can be tracked across different websites, across different sessions, across mobile and desktop," Acar says. "An email address is such a useful identifier for tracking, because it's global, it's unique, it's constant. Since the findings indicate that deleting data in a form before submitting it may not be enough to protect yourself from all collection, the researchers created a Firefox extension called LeakInspector to detect rogue form collection. And they say they hope their findings will raise awareness about the issue, not only for regular web users but for website developers and administrators who can proactively check whether their own systems or any of the third parties they're using are collecting data from forms without consent.

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

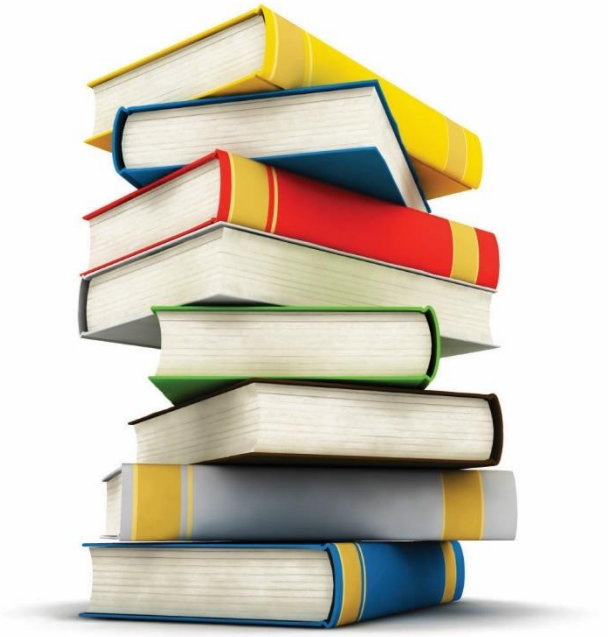
What did we learn? Do not enter your details unless you certainly agree to share them with the website. The decision must be made before the 1st strike not at Submit button.

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. Attackers Steal Money from PayPal Users

OMG – Even PayPal?



1 | June| 2022

"A security researcher claims to have discovered an unpatched vulnerability in PayPal's money transfer service that could allow attackers to trick victims into unknowingly completing attacker-directed transactions with a single click.

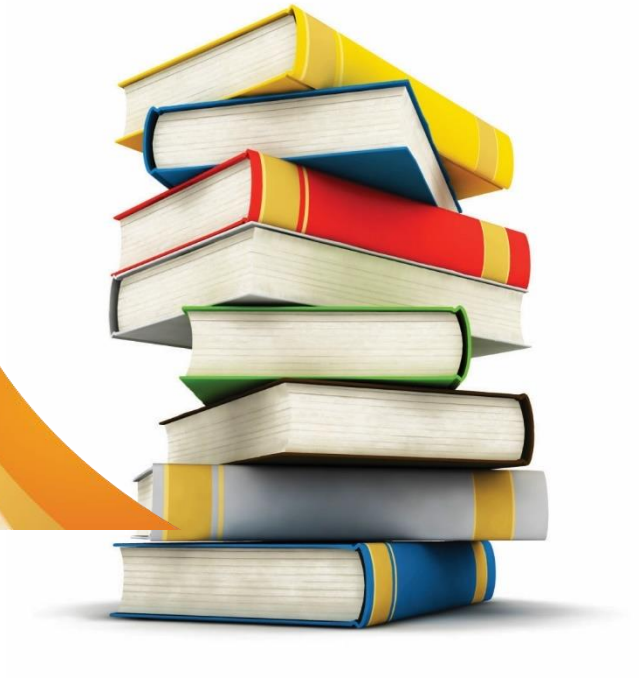
Clickjacking, also called UI redressing, refers to a technique wherein an unwitting user is tricked into clicking seemingly innocuous webpage elements like buttons with the goal of downloading malware, redirecting to malicious websites, or disclose sensitive information.

This is typically achieved by displaying an invisible page or HTML element on top of the visible page, resulting in a scenario where users are fooled into thinking that they are clicking the legitimate page when they are in fact clicking the rogue element overlaid atop it."
The story has been rectified to mention that the bug is still unpatched and that the security researcher was not awarded any bug bounty for reporting the issue. To Read the complete article.
What can you do? PayPal is still one of the more secured ways to pay, but as you see not perfect at all times. Review your monthly reports to ensure no one besides you used your PayPal account.

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 | June | 2022

6. Question from the previous newsletter:

Which of this best describes how criminals start ransomware attacks?

- **A. Sending a scam email with links or attachments that put your data and network at risk.**
- **B. Getting into your server through vulnerabilities and installing malware.**
- **C. Using infected websites that automatically download malicious software to your computer or mobile device.**
- **D. All of the above.**

The correct answer is "D" - Criminals will use all above mentioned methods.

New Question

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.**

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