How to Avoid Unprotected CyberDating?

Written by Alon Golan

Powered by odix

Table of Content

Meet the Author

Alon Golan

Alon's love story began amidst the hustle and bustle of Mexico City's busy streets. He was weighed down by a hefty 12-kilo laundry bag and sought assistance from an English speaker when he unexpectedly encountered his future wife. It was a chance encounter that would change the course of his life forever.

Alon Golan is a seasoned product marketing professional with over 10 years of experience in cybersecurity.

He's an avid technical storyteller with a keen eye for details. With his combined technical and creative background, he excels at translating complex technical concepts into well-articulated and compelling messaging that resonates with diverse audiences.

In his current role as Product Marketing Manager at odix,

Alon is focused on executing the company's go-to-market plan, the launch of new products and features, content creation, sales enablement collaterals, and positioning & messaging development that quantifies the value proposition.

Alon holds a Master's degree with dean's honors in Film and Media Production from the New York Film Academy. His perspective on life, work, and relationships is "make every day count".

When dating apps meet hackers

Cold February is THE month to search for love. As the online dating scene is blooming, it opens opportunities for hackers to act. Everyone knows a cyber incident is a real turn-off, and when love is part of the game, it makes it difficult to spot digital red flags.

In the quest for love, technology promised to shortcut the search for the significant other. But beware, the rise of online courtship has attracted the attention of threat actors, con artists, and players with malicious intent, hiding behind black hoodies and fake profiles. Protect your heart and avoid becoming another statistic digit. Learn how to spot digital red flags and navigate the rough water of the unprotected cyber dating scene.

First date: Keep the mystery and under-share information

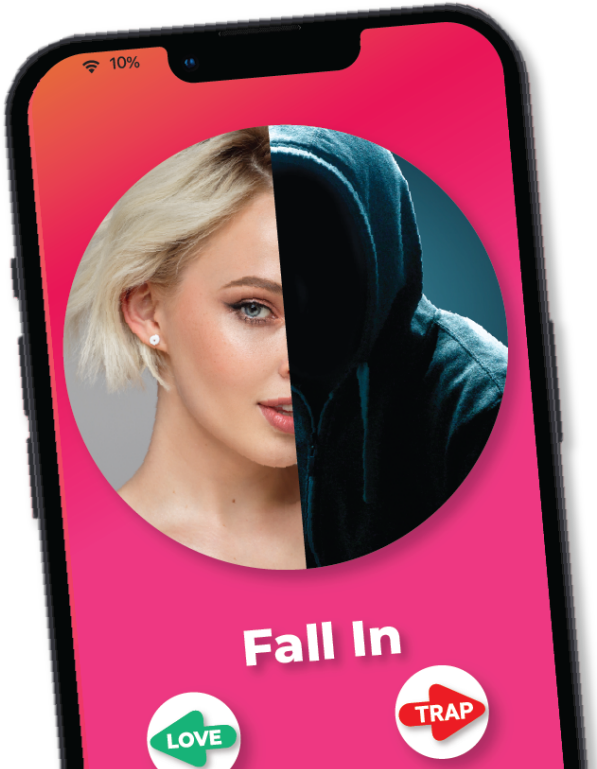
Who you are is your identity, and so is your data. You should be careful what you disclose and to which technology app you put your trust.

The Ashley Madison breach in July 2015 revealed the vulnerability of online dating sites. The lesson learned was that with enough resources and time, any system is breachable. While millions of users put their trust in dating apps to keep their private data private, the reality is that innovative hackers will eventually figure out a way into the system. That was the case with the world's most popular dating site, Tinder, when a threat actor managed to gain access to the system and see which profile pictures users have viewed, and to which direction they swiped. Moreover, threat actors gain the ability to track the user's physical location. With such information, consider a golden mine – hackers could leverage it for broad-scale blackmail and extortion attempts.

Private channels over the dark web and Telegram offer countless business opportunities for stolen private data from dating apps. Prices vary depending on the type and quality of information, such as email addresses, passwords, and credit card details. Sometimes you can even find sensitive medical information such as HIV and COVID-19 vaccination status. The price also depends on the date of the stolen data, with earlier dates commanding higher prices due to the lower likelihood of the credentials having been changed.

Social engineering is not socially friendly

On our way to finding true love, we share lots of information about ourselves creating a significant digital footprint that makes it so easy for hackers to leverage the data and create damage. Are you using the same credentials for all of your accounts? This makes their job even easier. The potential risk of data exfiltration goes from stolen Credit Card information, and identity theft, all the way to blackmail, shaming, extortion, and breaking a family household. Sophisticated hackers can lure romance seekers into engaging in a form of a video chat. In such cases the video can be pre-recorded, convincing the victim to engage in a sexual act. The session is then recorded and can be used later on for purposes of shaming, extortion, and blackmail.



> **To find true love we share lots of information, creating a significant digital footprint**

Love in practice: Two cents from a cyberdating veteran

Incorporate password management solutions to keep different passwords for each account. This way you have to memorize only one password.

Enforce a strong password mechanism that will include at least 12 characters, a combination of capital, lowercase, special characters, and numbers, and try to create a story that is logical only to you.

While not always possible to verify, ensure you're using a chat that supports and enables end-to-end encryption before disclosing private (or any) information.

Most apps and websites offer MFA (multi-factor authentication) as the default way for signing in. Use it. It will dramatically reduce the level of risk and identity theft.

Look for apps that guarantee immediate data deletion features. So at any point, you can get rid of any historical unwanted digital footprints.

When posting a profile picture, try to use a unique one that has never been shared before. Hackers can fairly easily use common tools to cross those pictures with another social platform account, and by doing so verify your actual identity.
Keep your sexy pictures old-school. If it's on a file it has potential slips into the wrong person. And with the association of pictures per person, the way to shaming, extortion, or blackmail is pretty near.

Spread love – not personal data

With the increasing rate of data sharing in the name of profit, and with hackers showing no mercy, it is time to conduct a serious debate on the way commercial companies take advantage of our private data in exchange for potential romantic hookups. While some application providers do their best efforts to protect users' data and integrity, the current situation is that hackers try even harder to breach any fence that is on their way and take control over digital assets.

2 The cost of falling in love

Online dating has become a popular way to meet new people, but with the rise in popularity comes the rise of privacy and safety concerns. From hackers using the information provided by users to cyber security breaches and sensitive content being sold as a commodity, there are many dangers to watch out for. In this article, we will explore these dangers and provide tips on how to protect your privacy and safety while using online dating services.

SCAMengers Hunt

Swindlers who specialize in romantic scams target love seekers across a variety of platforms. While seems to believe the threat is mainly focused on traditional dating websites, reports by the American Federal Trade Commission (FTC) demonstrate that scammers also prey on their victims on recreational and professional social media platforms. In fact, 40% of people who reported being deceived by a romance scam last year said that the initial contact occurred on social media, while 19% said it began on a website or app. Many people also reported that the scammer quickly diverted the conversation to other platforms like WhatsApp, Google Chat, or Telegram.

Real love can't remain virtual forever

If someone you meet online asks for money, a donation, or offers an attractive investment opportunity without meeting in person or with vague promises to do so in the future, that's a red flag. FCS's reports show that threat actors' excuses are often baked right into their fake identities. They may claim to be on a distant military facility or offshore oil rig or impersonate a successful person, investor, or entrepreneur. Those people are professionals who will sweet-talk their way into your pocket. If the situation seems too good to be true, or if a significant amount of time has passed without meeting in person, it's best to cut off communication. You might spend a few days sobbing into a pint of ice cream, but financial security is better than bankruptcy.

Unfortunately, the scam is unlikely to end there. Some criminals would maximize their efforts by publicly auctioning their victim's explicit content to the highest bidder over underground marketplaces

The cost of falling in love

According to a report conducted by the FTC in 2022, nearly 70,000 people reported falling victim to a romance scam, with reported losses totaling a staggering $1.3 billion.

Cybercriminals use sextortion to blackmail individuals for money or favors in exchange for not exposing their sexual content. Such data can be obtained using various channels; from hacked email accounts to planting malware inside an innocent-looking file, to using impersonation and social engineering tactics to trick people into willingly sharing it. “Revenge porn” is another common practice of sextortion. Studies show that younger people are more prone, with victims aged 18-29 over six times more likely to report sextortion than those 30 and over. In 2022, 58% of sextortion reports involved social media, with Instagram and Snapchat being the most common platforms.

Real love can't remain virtual forever

Love in practice: Two cents from a cyberdating veteran

- Use anti-malware tools to scan files, pictures, or videos provided by a potential romantic partner. These files could contain hidden malware.
- Always use discretion, common sense, and good judgment. If it's too good to be true- it's not true.
- Chat is great to exchange information - but if the partner on the other side seems overly avid to get sensitive information, or asks many questions over a short amount of time, it should raise some concerns.
- Does your loved one combine romance with any sort of cryptocurrency deal? It's time to move in a different direction.
- The American Federal Trade Commission also has a few useful tips and common practices to alert of:
- Nobody legit will ever ask you to help—or insist that you invest- by sending cryptocurrency, giving the numbers on a gift card, or wiring money. Anyone who does is a scammer.
- If someone tells you to send money to receive a package, you can bet it's a scam.

Broken Heart Recovery

According to the FBI, If you are a victim of a confidence/romance scam, they recommend taking the following actions:

Report the activity to the Internet Crime Complaint Center, your local FBI field office, or both. Contact IC3 at ic3.gov. Local FBI field offices can be found online at www.fbi.gov/contact-us/field.

Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.

Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.

Report the activity to the website where the contact was first initiated.

Spread love – not blank checks

Most people are genuinely looking for a life partner and dating apps do help people to find their soulmate. Don't let the fears of the next Tinder Swindler, hackers, fraud monsters, and other people with malicious intent draw you back. Listen to your gut and use every available tool that can be found online to ensure your first date wouldn't break your heart and your wallet.

3 Spread Love Not Blood

As the popularity of dating apps continues to rise, so do concerns around the privacy and security of users' data. More and more online love seekers acknowledge the risk of scams, fraud, and identity theft. It is being ranked among the top concerns by subscribers. But when there is a demand there's supply.

When AI is looking for (verified) love

To prevent the challenge of fake profiles, abuses, and fraud, a British-based company launched a dating app that requires the use of a full biometric ID and contains AI-powered image moderation technology to verify a profile's true identity. They fake the identity issue so seriously that as a requirement to log in to the service, every new subscriber must first identify themselves via a digital ID verification service whose clients include the NHS, the Post Office, the NUS, and other retailers.

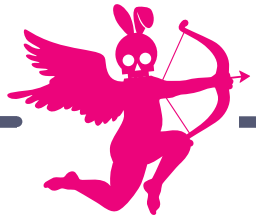
While some companies are taking a proactive approach to prioritize identity verification and integrity, it appears that others prioritize revenue over their users' privacy.

My App, My Data, My Terms of Use

Keeping users' private data by the application suppliers doesn't always happen, as some were caught in recent years selling users' data without their consent.

In 2018 the popular dating app "Grindr" was admitted to sharing its users' HIV status information with third-party organizations. Moreover, In 2020, a Norwegian Consumer Protection Authority report revealed that after scanning popular apps using a free online tool provided by the French non-profit organization Exodus Privacy), many dating apps, including Tinder and Grindr, sold their users' private data to third parties with commercial interest with the user's awareness. According to the report, the multitude of violations of fundamental rights is happening at a rate of billions of times per second, all in the name of profiling and targeting advertising.

This situation is particularly concerning for geosocial dating apps, especially those aimed at the LGBTQ community, as they create norms of oversharing personal information. In an article by Ari Ezra Waldman, Professor of Law and Computer Science at Northeastern University School of Law, he portrays how this oversharing culture creates a clear incentive for hackers and malicious actors to exploit users' personal data. The lack of sufficient protection and liability enforcement under current privacy and internet laws allows for the public disclosure of non-consensual intimate content, commonly referred to as "Revenge Porn". This creates a dangerous incentive for malicious actors and potential hackers to continue publishing such content.



> **Fundamental rights violations are happening at a rate of billions of times per second**

Due Diligence before Wine

Online dating also poses a darker side with dangerous consequences, such as meeting someone who may harm you. For instance, there have been reports of hate groups in certain Eastern European countries pretending to be LGBTQ community members to lure others into a meeting, leading to physical assault and online shaming. In 1997, an Israeli high school student was murdered by terrorists after being tempted by a woman he had been chatting with on ICQ.

Given the potential risks of an online affair gone bad, it is essential to take some precautions and gather objective information about the person you intend to interact with.

There are various practical checkups to indicate whether your potential date is legitimate or suspicious. Some internet red flags to look out for include a low number of connections on various social media platforms, signs of profile activity such as pictures, posts, comments, shares, and engagement with his or her friend list. It is also recommended to use a reverse image search on your match profile picture to rule out an association with a different profile. Additionally, some social behavior to watch out for include verifying the areas of interest mentioned in your match's profile by casually asking about them. For those in the paranoid department, there are more advanced alarm bells to consider, such as cross-referencing other people tagged in pictures of your date and checking their profile to see if they also store pictures of your match.

Love in practice: Two cents from a cyberdating veteran

- The American Federal Trade Commission has a few useful tips and common practices to alert of:
- Talk to friends or family about a new love interest and pay attention if they're concerned.
- Try a reverse image search of profile pictures. If the details don't match up, it's a scam.
- The American Federal Bureau of Investigation (FBI) recommends always double-checking a person's identity before meeting face-to-face. A great available method to do so is by using a "Reverse Image Search" tool to ensure the person's picture on the profile does not below someone else. To perform a reverse image search on profile photos:
- Right-click on the image and select "Search for an image."
- Right-click again and select "Save image as" to save the photo to your device.
- Using a search engine, choose the small camera icon to upload the saved image into the search engine.

Spread Love – not Blood

The convenience of online dating and socializing can be appealing. Ultimately, as adults, the choice of who we connect with depends on our best judgment. However, it's always wise to exercise some basic due diligence methods, share our findings with people we trust, and take necessary precautions. And remember, sometimes it's just better to randomly meet a person at the local coffee place, university, or via common acquittance.

Peace and Love to you and your Digital Self

About odix

odix develops and markets advanced anti-malware tools based on its patented Content Disarm and Reconstruction (TrueCDR™) technology for preventative cybersecurity in enterprises of all sizes. odix technology prevents malware infiltration into organizational networks by removing all malicious code from a wide range of file types. Uniquely, odix protects files from unknown attacks, where legacy solutions fall short.

odix solutions are trusted by enterprises in diverse sectors such as industrial, finance, insurance, government, and others. odix operates from its headquarters in Israel and regional offices in the U.S. and Europe.

To learn more about odix, visit odi-x.com

odix | MALWARE-FREE FILES