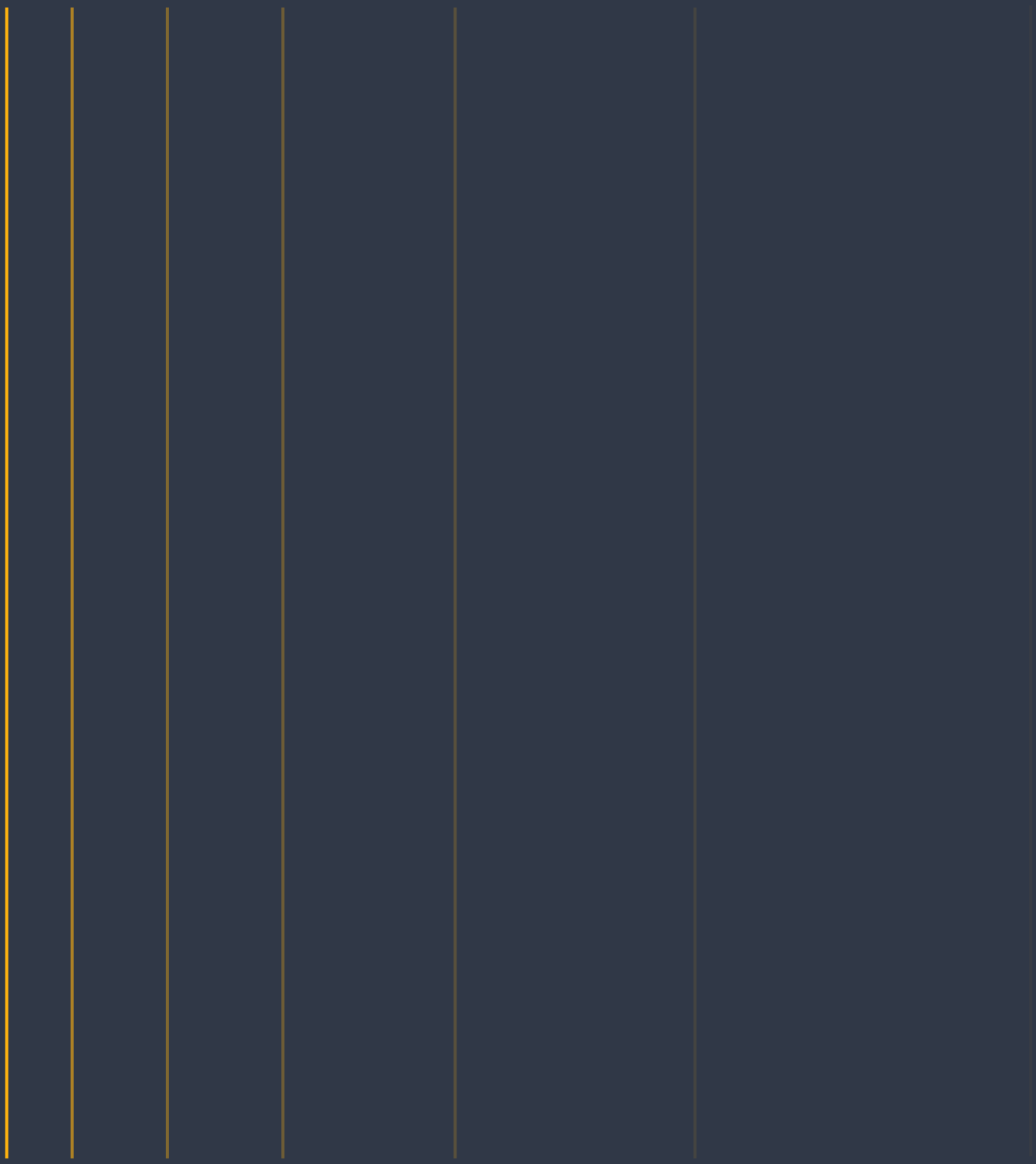
# How Fraud Relates to the Cyber Space

whitepaper

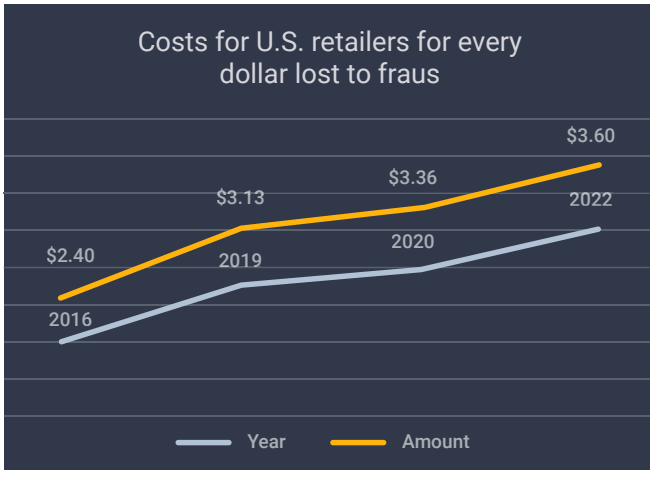


MALTEGO

# How Fraud Relates to the Cyber Space

## Financial Damage of Fraud and Levers to Combat Fraud

Virtually everyone in the developed world uses the internet, and every four out of five people worldwide admit to shopping online. Even if that only represents slightly over a quarter of the world's population, it's still quite impressive. ECommerce and Retail sector is set to see immense growth over the next decade or two. This means fraud will probably flourish, too. Retail ecommerce sales are set to reach $5.5 trillion in 2022. Currently, this represents about 21% of total retail sales worldwide. By 2025, it'll likely make up a quarter of the total. The problem is that ecommerce presents an excellent opportunity for Fraudsters to take advantage of less tech-savvy people—which means that the more popular ecommerce is, the more common online fraud will be. As successful fraud attempts rise, so do the number of financial losses incurred by both businesses and individuals. In the US alone, the amount lost to fraud in 2021 was over 5 billion dollars. The per dollar cost of ecommerce fraud on retailers has also continuously increased, from $2.40 in 2016 to $3.13 in 2019, $3.36 in 2020 and $3.60 in 2021. See the Chart below for more detailed view of fraud cost and its growth.




Furthermore, based on the Federal Trade Commission's Consumer Sentinel Report, the total amount lost to fraud in 2021 was $5,893,260,382 ($5.8 billion), an increase of more than 70% over the previous year. US retailers faced a 7.3% year-over-year increase in fraud costs and overall, it is estimated that online fraudsters will take more than $12 billion from businesses in 2022.

Money aside, fraud can also severely damage a company's brand, as 40% of customers state that they will blame the retailer for their accounts not being properly looked after. So, a business could actually lose its consumer base to top it all off. It is a vicious cycle that could heavily impact the economy in the long term.

## What are Typical Fraud Workflows?

With regard to fraud, we should differentiate between reactive and preventive measures. Reactive workflows are those which are taken once fraud has already been committed and, therefore, will need to be done under an intense amount of pressure, timewise. Preventive has more to do with company culture and habits, such as not opening spam emails, to prevent the crime before it occurs . With Maltego in particular, a preventive workflow is made up of due diligence, KYC, and attack surface management, among others.

### Preventive Measures

In most ideal cases, one would want to prevent the fraudulent activity before it even occurred. In this instance, preventive measures can be taken to protect your data from cybercriminals.

- **Risk assessment:** The first step one should take to prevent fraud is to test

fraud prevention security in your company. This will give you a clear indication of any possible "weak points" that may need addressing.

- **Use all the available tools:** Fight fire with fire and use technology to your advantage. Ensure that all systems are fully up to date, enable authentication and email filters, and make use of anti-phishing and anti-virus programmes.
- **Social media protocols:** Seeing as most hackers tend to gather information using social media, it is a good idea to place protocols on social media use in the office. This can include going as far as implementing blocks on certain websites which could be considered harmful.

### Reactive Measures

There are situations where fraud has, unfortunately, already taken place before you could do anything to prevent it. However, this is not the time to panic as there are certain reactive measures that can be taken in these cases.

- **Alert your team:** This should be done immediately, so that all parties are aware of the danger and can react accordingly.
- **Change passwords:** To halt any more harmful activity in its tracks, it would be advisable to change all passwords on accounts which have been harmed or threatened.
- **Implement additional authentication:** Now that the harm has already been done, it is a good idea to improve security wherever possible. For example, a two-factor authentication process could help shield from further attacks.

## How Fraud Relates to the Cyber-space

Cyber-Enabled Fraud and What it Entails

Internet fraud makes use of Internet-connected/enabled software and services to defraud and take advantage of victims. This type of crime can be done through a variety of methods, which separates it into a multitude of branches or types. Each type of fraud also has its own goals, some of which may overlap.

## The Types of Internet Fraud and their Goals

### Account Takeover (ATO)

ATO affects companies across all industries, from technology to financial sectors. This can technically fall under the umbrella of identity theft and phishing.. ATO fraud is when the criminal steals funds and/or personal information from user accounts via unauthorized access with stolen credentials. It is often a springboard into other types of crime, such as money laundering, identity theft, online scams, etc.

### Identity Theft

This is when someone's personal and financial information is illegally obtained to be used in fraudulent activities. In the cybercrime world, this is usually accomplished via ATO and phishing.

### Real-Money Trading (RMT)

RMT specifically affects the virtual economy as it tends to occur in the world of gaming, especially online. It is when a third-party ser-vice acts as a broker to sell a gamer's in-game items to other players for real money. This trade can also be done with in-game curren-cies. Technically, RMT is not an illegal activity as it falls under the umbrella of players' auton-omy. In most cases, RMT is seen as a good-will transfer, with a lot of trust involved. However, the problems come in when that trust is broken,

and the third-party broker does not hold up their end. In this case, the player would lose their items and in-game currency.

### Insider Threat

This is a threat or form of extortion that a company receives from someone within the company itself. People who could commit this crime are current or former employees, associates, or contractors. In other words, anyone who could potentially have access to important or confidential company information. This information can then be sold to a third party or ransomed. In the case of an accident (i.e., an employee's emails get hacked), the information could fall victim to a phishing attack.

### Returns Or Payment Fraud and Promo Abuse

Returns fraud is a fake claim made by a customer regarding a delivery or product, which they use to get money back. Payment fraud is when a customer does not pay for a product, they will usually send a fake proof of payment or pay multiple times without the money ever transferring. Finally, promo abuse is when a customer resells a discounted or promotional product at a highly inflated price.

### Fake Listings and Reviews

Fake listings prey on online customers, looking for certain items or services, by offering exactly what they may need with no intention of providing it. They usually ask for an upfront payment and, upon receiving it, "ghost" the customer. Fake reviews are an attempt to discredit a product, manufacturer, or service. This is a punishable crime according to the Federal Trade Commission and any person "using unfair or deceptive acts or practices in or affecting commerce" will be penalized. The reverse side of fake reviews is when a shady company will anonymously post positive reviews of themselves to trick customers into using their products or potential employees into applying for work.

### Affiliate Fraud

Affiliate fraud refers to any false or unscrupulous activity conducted to generate commissions from an affiliate marketing program. Affiliate fraud also encompasses any activities that are explicitly forbidden under the terms and conditions of an affiliate marketing program. In affiliate marketing, publishers and website owners can insert tracked links in their content that lead to a company's online store, product pages, and registration pages. When a specified action takes place, such as a registration or sale of a product, the affiliate is paid a commission. The temptation to profit from activity leads fraudsters to design ways to game the system with fake activity to generate new commission payments or increase the amount of the payments. Using stolen data for lead generation or stolen credit cards to generate sales. Affiliate fraud can be done with multiple ways:

- Typosquatting, or URL hijacking domains that are near those of the company's name or products to pick up a referral from the redirect.
- Getting people to download adware or spyware that inserts affiliate code automatically.
- Cloning other affiliate site's content to steal away traffic.
- Buying Google AdWords on the search terms where a company or its products are already ranked.
- Cookie stuffing all visitors to a website to profit if a visitor buys something later for unrelated reasons.

### Triangulation Fraud

Triangulation fraud is a means by which cybercriminals attempt to utilize stolen credit card

information within e-commerce marketplaces such as Amazon, eBay, Alibaba, and others.

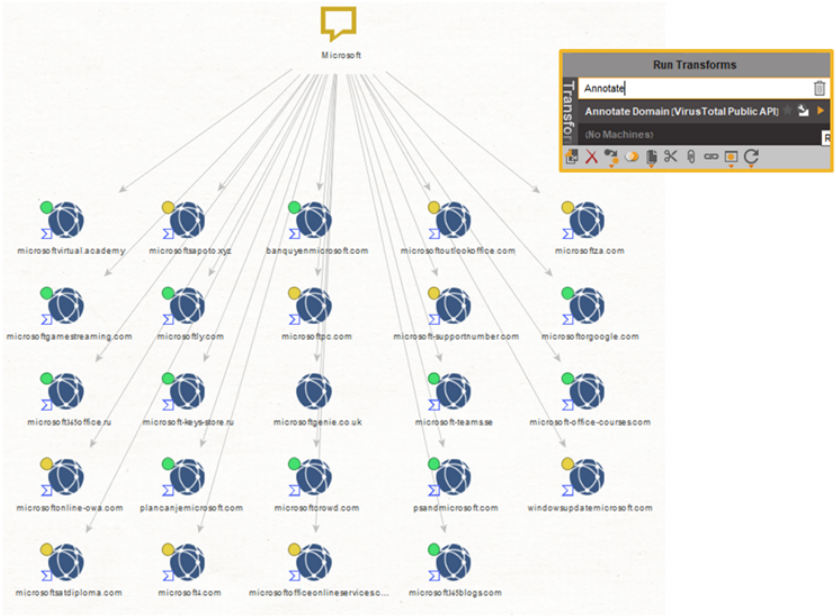
The scam is relatively simple: A fraudster possessing stolen credit card information lists items for sale on a fake online storefront. Oftentimes, the goods are listed at "too good to be true" prices to lure buyers in. Once a customer makes the purchase, the fraudster will purchase the same item from a legitimate seller using the stolen credit card information, routing the goods to the customer's address.

In the end, the customer has unknowingly received stolen goods and the legitimate merchant has been left with payment from a fraudulent card, causing a wide range of issues on their end.

## How to Use Maltego to Combat Fraud

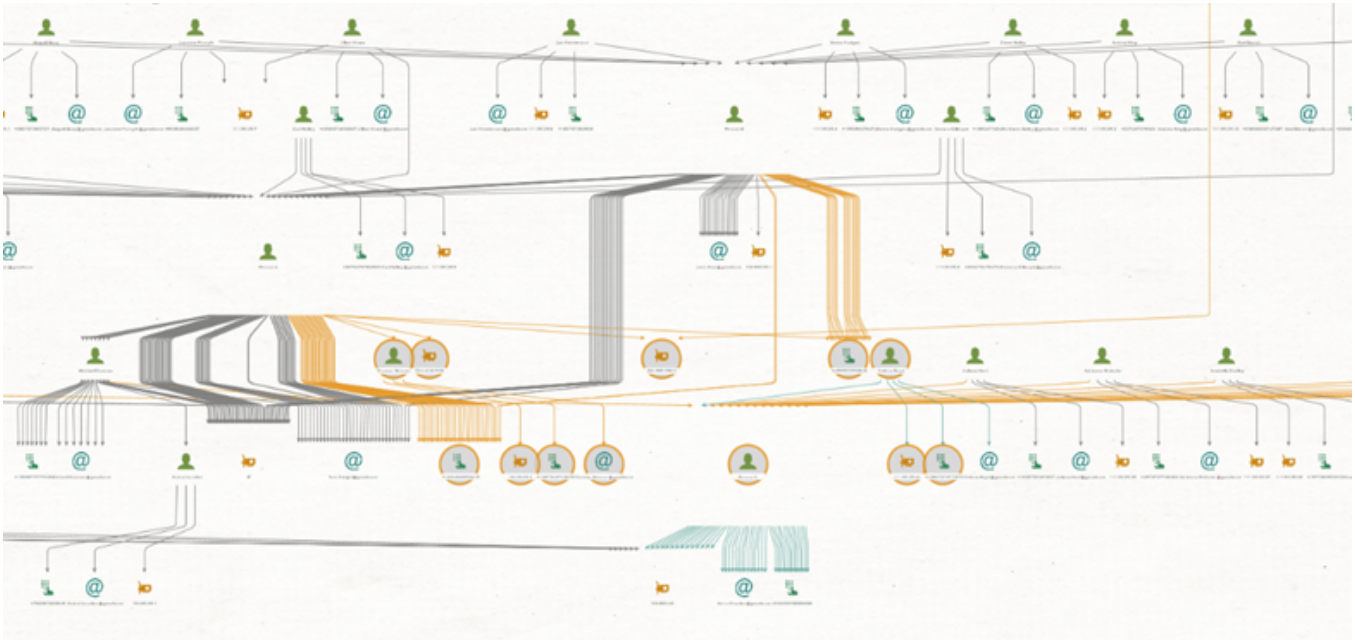
Maltego is a key player in combatting fraud online. As a virtual mapping tool, Maltego is on the forefront of using accumulated data to narrow down a search field.

One way this can be done is through a proactive or reactive investigation of potential phishing sites that might be targeting your customers to steal their identity by forging your brand in fake websites. Fraudulent websites can be identified with some data sources such as Scamadviser, WhoisXML API, and DomainTools. Identified websites can be further analyzed to identify if they have been marked as malicious or suspicious by different reputational engines, such as Virustotal, find out websites or social media posts that might be linked to them and map the infrastructure for a proper takedown process.



Another way is through geospatial link analysis, which, through the use of Google Geocoding Transforms in Maltego, allows analysts to find and identify global patterns more easily. Even phone numbers can be investigated with OpenCNAM and IPQualityScore, which aids in the search for people of interest within fraud cases .

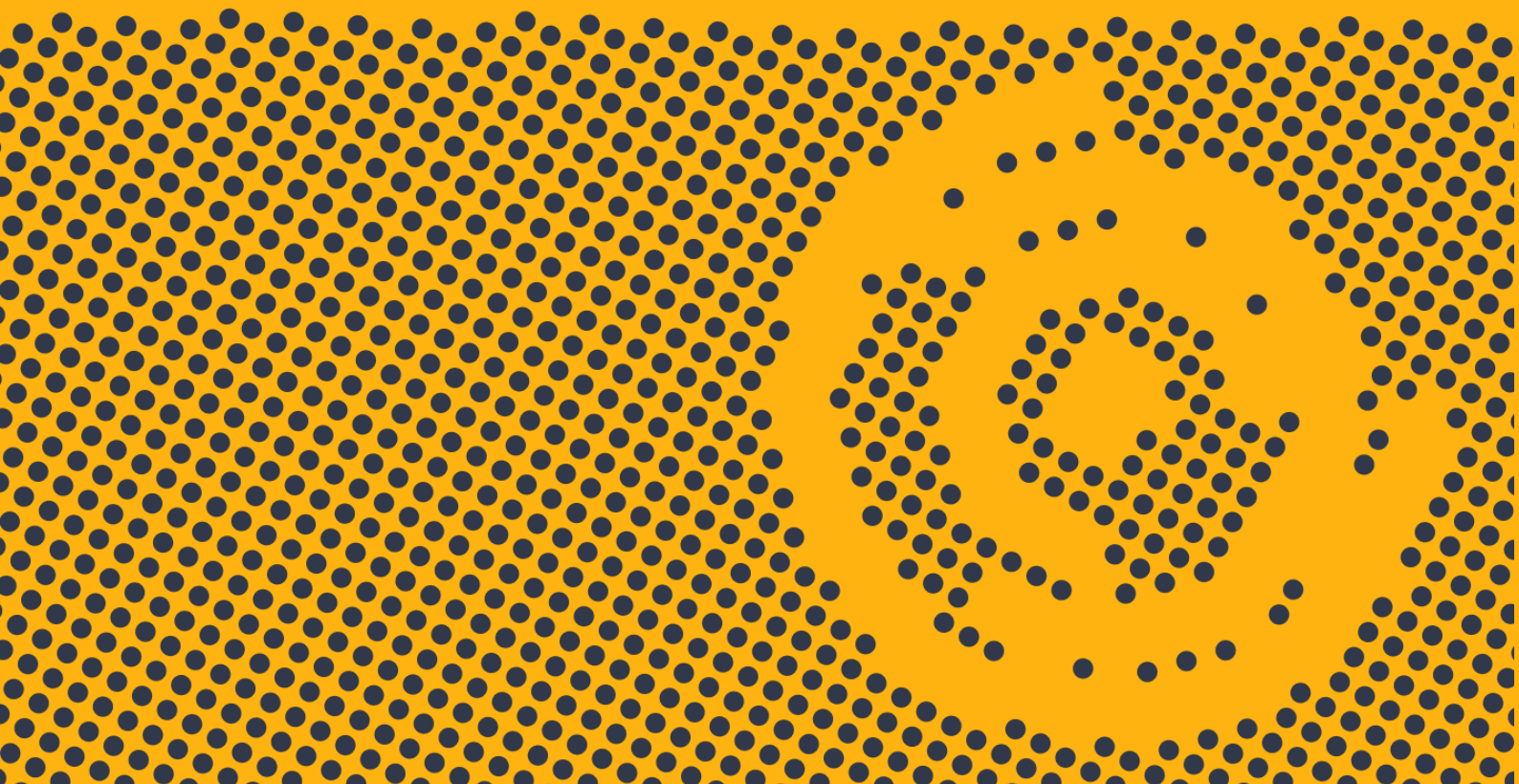
Furthermore, Maltego can be used as analysing and mapping tool for fraudulent and suspicious activities, finding patterns and connections among different type of internal or external data involving IP addresses, emails, phone numbers, dates, credit card holder names, domains, phishing websites and any other digital footprints of users who lands on Ecommerce store websites.



For more information, please visit
maltego.com

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

# MINE • MERGE • MAP / DATA



whitepaper

Maltego Technologies GmbH
Address: Paul-Heyse-Strasse 29, 80336 Munich
Email: contact@maltego.com
Phone: +49-89-24418490

MALTEGO