Identify your weaknesses before they can be exploited by malicious actors.

MACFTD is widely recognized as a leading organization in the field of cybersecurity, offering innovative solutions and expertise to help protect businesses and individuals from online threats.

We pride ourselves on providing a premium level of protection and service to our clients, ensuring their peace of mind and safeguarding their digital assets with the highest level of care and expertise.

-----------------------------------------------------------------------------------------------

We are dedicated to serving you and meeting your needs through our wide range of popular services, designed to provide optimal solutions and support for your business or personal cybersecurity requirements.

Services

1

**Our Vulnerability Assessment and Penetration Testing (VAPT) services are highly sought-after, providing comprehensive and thorough evaluations of your systems and networks to identify potential weaknesses and fortify your defenses against cyber threats.**

A Vulnerability Assessment is a quick automated examination of network devices, servers, and systems to identify fundamental vulnerabilities and configuration issues that an attacker may be able to take benefit off. It is generally conducted within the network on internal devices.  
  
A Penetration Test is an in-depth expert-driven activity focused on pinpointing various potential routes an attacker could use to break into the network. In addition to the vulnerabilities, it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter.

Our VAPT services are designed for businesses of all sizes and industries, as well as individuals seeking to secure their personal digital assets. Any organization or individual looking to safeguard their network and data from cyber threats can benefit from our comprehensive and effective VAPT solutions.

Our VAPT services test a wide range of network devices, servers, and systems to identify potential vulnerabilities and configuration issues that could be exploited by cyber attackers. We conduct in-depth assessments of your network infrastructure, web applications, and wireless networks, as well as testing for social engineering and physical security weaknesses, providing a comprehensive evaluation of your overall security posture.

Our VAPT services cover a comprehensive range of testing techniques, including reconnaissance to gather valuable information about the target organization, testing for default credentials or misconfigured servers, injection attacks to replicate external attacker behavior, and identifying vulnerabilities in authentication and session management mechanisms. We also test for sensitive data exposure and server security misconfigurations, and identify potentially exploitable unpatched services. Our expert team tests for broken authentication and session management, as well as insufficient security configurability, to ensure that all possible vulnerabilities are identified and addressed.

Services

2

**Our Mobile Application Penetration Testing services provide comprehensive testing and evaluation of mobile applications to identify and address potential security vulnerabilities.**

Our expert team uses industry-leading techniques and tools to assess the security posture of your mobile applications, including testing for data leakage, authentication and session management weaknesses, and identifying potential vulnerabilities in the code. We provide in-depth reporting and remediation recommendations to ensure that your mobile applications are secure and protected against cyber threats.

Our Mobile Application Penetration Testing services take a comprehensive approach to identifying security vulnerabilities in mobile applications, focusing on six key areas: architecture and design, communication, data storage and privacy, authentication and authorization, misconfiguration issues, and underlying API vulnerabilities. We thoroughly assess the application's design and architecture for potential security issues, including intercommunication of different logical components. Additionally, we test for communication vulnerabilities to ensure that sensitive data is not transmitted over unencrypted connections. We also check for clear text storage of sensitive information and identify any authentication and authorization issues, including the possibility of 0-click or 1-click account takeovers. Misconfiguration issues in third-party services or libraries and within the application itself are also identified, including improper handling of debug messages and error codes that may reveal internal information to end-users. Lastly, we perform API security testing on the underlying API consumed by the mobile application, identifying web vulnerabilities such as XSS, SQLi, information disclosure, and privilege escalation.

Services

3

**Infrastructure Penetration Testing: Protecting Your Network and Systems.**

Our Infrastructure Penetration Testing services are designed to comprehensively evaluate your network and systems, identifying potential vulnerabilities and weaknesses that could be exploited by cyber attackers. Our expert team reviews security principles, network solutions, traffic flows, and security solutions to prepare your organization and network infrastructure for potential threats. We conduct external and internal vulnerability scans to identify potential weaknesses in your IT ecosystem and network, and scan your relative tech stack to provide more precise results. To ensure the accuracy of our testing, we use trusted community tools and open-source software, which are thoroughly tested to ensure that they do not damage your network systems. Our goal is to provide you with comprehensive and actionable insights to help you fortify your network and protect against cyber threats.

Our Infrastructure Penetration Testing services involve a range of testing techniques to comprehensively evaluate your network and systems for potential vulnerabilities and weaknesses. We perform port scanning, host discovery, and check for known vulnerabilities and default misconfigurations that could lead to insecurities. We also use input fuzzing to identify potential security issues and test for the OWASP API Security Top 10 Vulnerabilities of 2020, including broken object level authorization, broken authentication, excessive data exposure, lack of resources and rate limiting, broken function level authorization, mass assignment, security misconfiguration, injection, improper assets management, and insufficient logging and monitoring. Our testing helps to identify potential areas of data compromise and disclosure, unpatched domains and servers, incorrectly configured database servers, and servers/applications vulnerable to default credential attacks. We validate high-severity results through a manual verification process to ensure accuracy and provide you with actionable insights to help you fortify your network and protect against cyber threats.

Services

4

**Our Vulnerability Scanning services provide comprehensive automated scanning of your network and systems to identify potential vulnerabilities and weaknesses. Using industry-leading tools and techniques, we perform regular scans to ensure that your systems are up-to-date and secure, providing you with actionable insights to help you protect your network against cyber threats.**

Our Vulnerability Scanning services are designed to help organizations identify potential security vulnerabilities in their network and systems, both internal and external. This automated high-level testing is ideal for organizations that want to continually monitor and test their applications and infrastructure to catch vulnerabilities before they become a security issue. While vulnerability scanning and penetration testing are often confused, vulnerability scanning is an automated process that identifies vulnerabilities, while penetration testing is a more exhaustive examination that includes manual testing to exploit weaknesses in your systems.

Our methodology involves conducting external and internal vulnerability scans to identify potential vulnerabilities in your IT ecosystem, with a focus on identifying vulnerabilities inside the network that may not be exposed by external scans. We also scan using community tools and specific tech stacks for greater accuracy and precision. Additionally, we use private and public tools to look for common vulnerabilities in web applications, including injection flaws, cross-site scripting, and other vulnerability classes arising from insecure code.

Our vulnerability scanning services offer several benefits, including reducing the attack surface of your organization, providing ongoing and updated assurance, and contributing to meeting data protection requirements. Our quick and frequent vulnerability scanning services provide detailed reports with easy-to-follow remediation advice, enabling you to quickly address any vulnerabilities and protect your network against cyber threats.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Services

5

**Our API Security Testing services provide comprehensive testing and evaluation of the security of your APIs to identify and address potential vulnerabilities. Our expert team uses industry-leading techniques and tools to assess the security posture of your APIs, including testing for common vulnerabilities such as injection flaws, broken authentication and authorization, excessive data exposure, and more. We provide in-depth reporting and remediation recommendations to ensure that your APIs are secure and protected against cyber threats.**

API security testing is a critical process for any organization, as it helps to identify and address potential vulnerabilities in your APIs. This testing involves assessing the security, correctness, and reliability of the endpoints of your application program interface (API), to ensure that it complies with security best practices and mitigate any potential security gaps.

Our API security testing services are designed for organizations that are running REST, GraphQL, and SOAP APIs, whether they are integrated into their web application or offered as a separate API service to their customers. Our methodology involves both static and dynamic analysis, with the majority of our focus on dynamic API security testing. This involves sending active requests to the API to surface potential vulnerabilities based on the response received from the API. Our testing covers input fuzzing, the OWASP API Security Top 10 Vulnerabilities of 2019, API logic testing, and excessive role-based testing.

API security testing offers numerous benefits, including identifying missing API service method configurations, providing real-time awareness of threats associated with your APIs, proactively identifying and detecting software security issues in APIs before they are deployed to production environments, and identifying and fixing authorization and authentication vulnerabilities. With our comprehensive API security testing services, you can ensure that your APIs are secure and protected against cyber threats, giving you and your customers peace of mind.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Services

6

**Our Access Control Model Evaluation services provide comprehensive testing and evaluation of the access control model of your system, with a focus on role-based testing. Our expert team uses industry-leading techniques and tools to assess the security posture of your access control model, including testing for potential privilege escalation scenarios and identifying any weaknesses in the design and implementation of the system. We provide in-depth reporting and remediation recommendations to ensure that your access control model is secure and protected against cyber threats.**

Sure! Access control is the practice of controlling access to resources or functionality in a system based on a user's identity and privileges. A flawed access control scheme can have devastating consequences, such as unauthorized access to sensitive information or even complete takeover of the system.

MACFTD offers a Role-Based Testing Service specifically designed for SaaS businesses that utilize Role-Based or Access-Control technologies in their applications. This service is aimed at applications that allow customers to invite new members to their tenants/organizations with limited permissions.

MACFTD uses a proper methodology to test access control models in a modern way. Their methodology covers all the scenarios that can lead to privilege escalation within the target system and provides full coverage of the target model. MACFTD has different techniques for each kind of privilege escalation scenario that can arise within the system.

Their three main effective techniques/approaches are the Forward Approach, Backward Approach, and Mixed Approach. In the Forward Approach, a user is invited with only one permission and then tries to access all other restricted API endpoints in sequential order. In the Backward Approach, the user is granted all the permissions in the model except one permission, and they try to access the respective API endpoint of the devoid permission. The Mixed Approach involves inviting a user with a set of mixed permissions from the permission list, and then they try to access the corresponding API endpoints of restricted roles.

By using MACFTD 's service, you can identify privilege escalation in your web-app/API, get full insights into your access control models, identify permission overrides in your web-app/API, get customized reports to help you understand the privileges set around different roles in the application, and understand different roles and the damage that can be done when privilege escalation happens.

Overall, MACFTD 's Role-Based Testing Service is a great way to ensure that your access control model is properly implemented and secure.

Services

**7**

**Continuous Security Testing**

**Traditional penetration testing is not enough to ensure the safety of your system against online threats, especially for large application estates or applications that change frequently. This is because it's not practical to perform pen-tests every few years and believe that you're safe against online attacks. Moreover, new vulnerabilities can be introduced into your application every day by pushing new code to production or making changes to existing code. Therefore, a new approach is needed that delivers continuous security testing solutions that can scale. This is where our Continuous Security Testing (CST) service comes in.**

**Our CST service is designed for organizations that want to continually test their applications and infrastructure to catch vulnerabilities before they cause an issue. This includes companies that often push code to their production servers because every time code on the server changes, it can affect the application logic, tech stack, dependencies, and infrastructure that the applications are hosted on. Our CST service allows you to continually test your applications and infrastructure to keep an eye on any new vulnerabilities introduced to your network or application.**

**We use a methodology where we test your product every week/month or after a specific time-gap, and we provide you with a weekly/monthly summarized report that includes different types of attacks and test-cases that your application has gone through. This brings both new vulnerabilities and quick insights into the test-cases your product has gone through.**

**Our testing services include web application vulnerability assessment and penetration testing, mobile application penetration testing, access control model evaluation (role-based testing), infrastructure penetration testing, vulnerability scanning, and API security testing.**

**The benefits of our CST service include continuous surveillance on your application and network security, continuous attack surface management, balanced vulnerability reporting, and cost efficiency. To learn more, you can visit our blog**

Services

**8**

**Code Review**

**Code review is an essential process in cybersecurity that helps ensure that software is secure and reliable. During code review, a team of security analysts reviews the source code to identify any potential vulnerabilities and ensure that the code follows best practices for secure coding. This process can include testing the code for vulnerabilities, examining the code for the use of known insecure functions or libraries, and reviewing the code for the implementation of security controls such as input validation and output encoding.**

**Dynamic analysis, also known as runtime analysis, is a critical component of code review. It involves analyzing code as it is being executed to identify issues that may not be apparent from static analysis alone. Our consultants use a combination of static and dynamic analysis techniques to conduct code reviews, including reviewing the code manually, using automated static analysis tools, and testing the code with different input values.**

**Code review is suitable for organizations of all sizes that want to improve the security and reliability of their software. It is especially important for companies that handle sensitive data or operate in regulated industries as it can help ensure compliance with relevant regulations and standards. By identifying and addressing potential issues early on, organizations can improve the reliability and security of their software, which can lead to cost savings and improved efficiency.**

**The benefits of code review include improved security, enhanced reliability, increased efficiency, enhanced maintainability, and improved compliance. By identifying and addressing potential issues early on, organizations can reduce the risk of costly bugs or vulnerabilities, improve the quality of their software, and gain a competitive advantage**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Services

**9**

**☁️ Cloud Security Testing**

**Cloud security assessment is a vital process that involves evaluating the security of an organization's cloud environment, including its infrastructure, applications, and data. This process helps to identify potential security weaknesses and vulnerabilities, which can be addressed to improve the overall security of the cloud environment.**

**Our cloud security assessment services are designed to assist organizations in understanding the risks and vulnerabilities associated with their cloud environment. Our team of security experts will conduct a thorough review of your cloud environment, including infrastructure, applications, and data, to identify any potential security weaknesses. By choosing our services, you can gain a better understanding of the security of your cloud environment and take the necessary steps to protect your data and systems.**

**Our methodology for conducting a cloud security assessment involves several steps, including planning and preparation, threat modeling, testing, analysis, reporting, and remediation. During the testing phase, we evaluate various aspects of the cloud environment, such as infrastructure, access controls, data security, application security, network security, and compliance. Once the testing is complete, we provide a detailed report that includes the results of the testing, any security issues that were discovered, and recommendations for addressing them.**

**The benefits of cloud security assessment include improved security, enhanced compliance, increased efficiency, reduced costs, and improved user trust. By identifying and addressing security vulnerabilities, organizations can prevent data breaches and other security incidents, avoid fines and penalties, reduce downtime and disruptions, and build trust with their users and customers.**

**In summary, cloud security assessment is an essential process for any organization that uses cloud computing. It helps to ensure the security of the cloud environment and protect against potential cyber threats, ultimately leading to increased business success and user trust**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**🔐 Our Penetration Testing Services.**

**Certainly! Penetration testing involves simulating real-world attacks against your digital system to identify vulnerabilities and assess the potential security risks. It's an essential step towards ensuring the security of your system and protecting against potential threats.**

**The vulnerability classes that your penetration testing services cover are wide-ranging and comprehensive. For instance, default credentials issues can occur when default usernames and passwords are not changed, leaving the system vulnerable to attack. Injection attacks can be used to exploit vulnerabilities in input fields, and broken authentication and session management can enable attackers to gain unauthorized access to your system.**

**Server security misconfiguration, unpatched services, and insufficient security configurability can also leave your system vulnerable to attacks. Client-side vulnerabilities such as XSS, CSRF, and CORS misconfigurations can be used to steal sensitive information or take control of a user's session.**

**Penetration testing can also uncover business logic issues, infrastructural issues such as HTTP request smuggling and cache deception, file upload vulnerabilities, privacy violation issues, insecure randomness issues, cryptographic issues, default misconfiguration issues, privilege escalation issues, and sensitive/excessive data exposure vulnerabilities.**

**Overall, your penetration testing services cover a wide range of potential vulnerabilities and security issues, which can provide peace of mind to your clients by identifying and mitigating potential risks before they can be exploited by attackers.**

**One of the best ways to evaluate the security of your system, find vulnerabilities, and assess the risk that any existing vulnerabilities pose in the real world is through penetration testing.**

**Our penetration testing services ensure that your digital system is tested for the following vulnerability classes.**

**✅ DEFAULT CREDENTIALS ISSUES**

**✅ INJECTION ATTACKS**

**✅ BROKEN AUTHENTICATION AND SESSION MANAGEMENT**

**✅ SERVER SECURITY MISCONFIGURATION**

**✅ UNPATCHED SERVICE**

**✅ BROKEN AUTHENTICATION AND SESSION MANAGEMENT**

**✅ INSUFFICIENT SECURITY CONFIGURABILITY**

**✅ CLEINT SIDE VULNERABILITIES (XSS,CSRF,CORS MISCONFIGRATIONS ETC)**

**✅ BUSINESS LOGIC ISSUES**

**✅ INFRASTRUCTURAL ISSUES (HTTP REQUEST SMUGGLING, CACHE DECEPTION ETC)**

**✅ FILE UPLOAD VULNERABILITIES**

**✅ PRIVACY VIOLATION ISSUES**

**✅ INSECURE RANDOMNESS ISSUES**

**✅ CRYPTOGRAPHIC ISSUES**

**✅ DEFAULT MISCONFIGURATION ISSUES**

**✅ PRIVILEGE ESCALATION ISSUES**

**✅ SENSITIVE/EXCESSIVE DATA EXPOSURE VULNERABILITIES**

**We offer end-to-end solutions for all your programming, application, maintenance, and network needs, from A to Z.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**At MACFTD, we strive to deliver top-notch cybersecurity solutions that fortify your critical networks and safeguard your valuable data, all at a cost-effective price point.**

**MACFTD is a prominent and trusted provider of state-of-the-art cybersecurity solutions that cater to the needs of businesses of all sizes. Their specialized services include information security, maintenance, and electronic services, all designed to offer comprehensive protection for their clients' valuable data from cyber threats. What sets MACFTD apart is their team of dedicated experts who are committed to delivering the highest level of security and support to their clients. They leverage innovative technology and a proactive approach to cybersecurity to help their clients stay ahead of the constantly evolving threat landscape. With MACFTD as a trusted partner, businesses can be confident in the integrity and confidentiality of their sensitive information.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Our company has played a crucial role in identifying and resolving a significant number of vulnerabilities, having successfully assisted in the discovery and remediation of over 1937 security threats..  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Contact Us Now**

Don't hesitate to reach out to us today to benefit from our exceptional server security service. Our goal is to provide you with an accurate configuration and robust protection for your servers, applications, infrastructure, and customer data, all of which are essential for achieving optimal performance for your business. Let us help you safeguard your critical assets and keep your operations running smoothly. Contact us now to get started.

**\_\_\_\_\_  
FREQUENTLY ASKED QUESTIONS**

**What is Pentesting?**

**A pentest, short for penetration test or intrusion test, is a type of security audit performed on a computer system. The goal of a pentest is to identify potential vulnerabilities in the system that could be exploited by cybercriminals to gain unauthorized access. By simulating a real-world attack, pentesters can help organizations assess the effectiveness of their security measures and identify areas that need improvement. Overall, the aim of a pentest is to ensure that the system is as secure as possible and that sensitive information is protected from unauthorized access.**

**Why should i do pentesting?**

**Cyber attacks are a growing threat in today's digital age. It's possible to be targeted and attacked without even realizing it, and the consequences can be devastating. Not only can cyber attacks result in financial losses for a company, but they can also damage a company's reputation and erode customer trust. Therefore, it's crucial to take proactive measures to protect against cyber attacks. By conducting regular security audits and penetration testing, organizations can identify and address vulnerabilities before they can be exploited by cybercriminals. Prevention is always better than cure, and the investment in cybersecurity measures can help save thousands of euros in potential losses. So, it's important to be proactive and take the necessary steps to protect your company's sensitive information and data.**

**What are the benefits of pentesting my business ?**

**Performing a penetration test, or pentest for short, is an excellent way to enhance your business's security. A pentest can help you identify vulnerabilities in your systems, understand how they can be exploited, and assess the risks associated with those vulnerabilities. By addressing these vulnerabilities, you can better protect your infrastructure, achieve higher security standards, and preserve the confidentiality of your data. A pentest also helps you control against unauthorized access and improper use of your data, protects against the loss and leaking of sensitive information, and prevents intrusion and tampering with your network. Overall, a pentest is a valuable tool for maintaining data discretion and ensuring the safety of your business.**

**What type of box (black / grey / white) is best suited to my business?**

**The three types of audits can be beneficial for any type of business. However, at Open Data Security, we offer personalized advice to help you determine which type of audit is most appropriate for your specific needs. We encourage you to reach out to us for assistance in making the best decision for your business.**

**What resources or access are required to conduct a pentest?**

**The resources and access required for a pentest will vary depending on the type of audit being conducted. In certain cases, we may not even need access to any data. To learn more about the specific requirements for your pentest, please feel free to contact us.**

**How long does it take to perform a pentest?**

**The time required to conduct a security audit will vary depending on the unique circumstances of each case. For more information on estimating the timeline for your specific audit, please don't hesitate to reach out to us.**

**Once the problem / security gap is located, how long would it take to fix it?**

**The time required to remediate a security breach will depend on the type and severity of the breach. Each security incident is unique and requires a tailored approach to effectively address the issue. Our team can provide guidance on how to efficiently and effectively resolve security failures. Please don't hesitate to contact us for more information.**

**I have a small business, should I do a pentest too?**

**It is highly recommended to conduct a pentest if your business uses any type of access system, whether it be internal or external, and manages data that should be kept private. No system is completely immune to cyber attacks, and any business can become a target for cyber criminals. A pentest can help you identify vulnerabilities in your systems and take proactive measures to enhance your overall security posture. At Open Data Security, we are here to help you safeguard your business and protect your valuable data. Don't hesitate to contact us to learn more about how we can assist you.**

**How often should I do a pentest?**

**Performing a security audit every time a software or application is updated is highly recommended to ensure that any newly introduced vulnerabilities are identified and addressed. At a minimum, it is advisable to conduct a security audit once a year to proactively assess your overall security posture and identify any potential vulnerabilities. Our team at Open Data Security can assist you in conducting regular security audits to help you stay ahead of potential threats and protect your valuable data. Please feel free to contact us to learn more.**

**How do I send you the accesses / resources you need to carry out the pentesting?**

**The access and resources will be sent confidentially through a secure way, always respecting the privacy of your data.**

**Once the problem is solved, am I protected against future threats?**

**Every day new updates appear in the systems, changing the security parameters of their infrastructures which can generate new security breaches. At Open Data Security we recommend you to keep certain security protocols to avoid it and to always have on your side cybersecurity experts who guarantee the security of your company at all times. On the other hand, we must bear in mind that cybercriminals also use social engineering to gain access to your systems, and it is something that does not depend solely on the level of security of your infrastructures.**

**I already made a pentest in the past, is it necessary to do it again?**

**Of course. Every time you perform an update on your systems you should check that they are still safe. Also, if the last time you did a penetration test was more than a year ago, you should perform another one again.**

**ABOUT US**

. MACFTD is a leading provider of cybersecurity solutions for businesses of all sizes. Our mission is to provide our clients with top-notch security measures that protect their critical networks and data from any potential cyber threats. We offer affordable services that are tailored to meet the unique needs of each client, and we provide direct support to help eliminate any security vulnerabilities. With MACFTD, you can rest assured that your digital assets are safe and secure from any and all cyber attacks.

**At MACFTD, we understand that security testing is a critical component to ensure the protection of your digital assets against potential cyber-attacks. In today's digital landscape, security services have become increasingly important, and we recognize the high demand and value that they hold. That's why we are dedicated to making top-quality security services accessible to businesses of all sizes at reasonable prices. Our team of experts is highly skilled in testing online assets for security vulnerabilities, and we are committed to providing our clients with the peace of mind that comes with knowing their digital assets are secure. With MACFTD, you can enjoy the benefits of online security without breaking the bank.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Our Social Networks**

[**WWW.MACFTD.COM**](http://WWW.MACFTD.COM)

[**https://www.linkedin.com/company/macftd/**](https://www.linkedin.com/company/macftd/)

[**https://www.facebook.com/profile.php?id=100091521781686&sk=about**](https://www.facebook.com/profile.php?id=100091521781686&sk=about)

[**https://www.instagram.com/macftdsa/**](https://www.instagram.com/macftdsa/)

[**https://twitter.com/MACFTD**](https://twitter.com/MACFTD)

[**https://github.com/macftd**](https://github.com/macftd)

[**https://t.snapchat.com/v8PlIzpr**](https://t.snapchat.com/v8PlIzpr)

[**macftdsa@gmail.com**](mailto:macftdsa@gmail.com)

[**http://www.tiktok.com/@macftd**](http://www.tiktok.com/@macftd)

[**https://www.youtube.com/@MACFTD/about**](https://www.youtube.com/@MACFTD/about)

Support Team: [support@macftd.com](mailto:support@macftd.com)

Sales Team:

[sales@macftd.com](mailto:sales@macftd.com)

CEO| Founder: [imran@macftd.com](mailto:imran@macftd.com)

CEO | Founder: [adelalnoob@macftd.com](mailto:adelalnoob@macftd.com)

Phone (SA): +966540000804

Phone (UK): +442034328195

Phone (IN): +917780908136