TECHNOLOGY NEWSLETTER

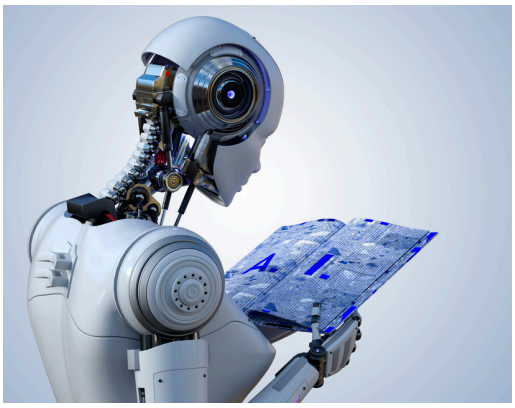
THE MISSON OF THE LADD TECHNOLOGY DEPARTMENT

To provide high quality, secure, and efficient IT solutions that enable LADD to provide better services to the people supported and all stakeholders to achieve the Mission, Vision and Values of LADD and administrative objectives.

Information technology is critical for LADD's mission and its successful operations. Information technology is needed to create a strategic advantage for LADD. When information technology initiatives align with the strategic goals of LADD, the impact can be transformative – empowering staff to enhance the quality of life for all we serve, improving LADD's operations to deliver quality services, and fomenting improvement through the intelligent use of data.

THE FUTURE OF ARTIFICIAL INTELLIGENCE

AI is fundamentally changing everything! AI is no longer a futuristic technology; it's the present and future of innovation across industries. AI is fundamentally reshaping how businesses operate. It's optimizing workflows, reducing costs, and solving problems that were once thought unsolvable.



ARTIFICIAL INTELLIGENCE - CONT.

However, adapting to this AI-native era is critical. Organizations that embrace AI will thrive, while those that hesitate risk falling behind. The transformative power of AI lies in its ability to bridge the gap between manual and fully autonomous processes. This shift will impact not just cybersecurity but every facet of business operations.

Unfortunately, AI's power isn't limited to defenders—cybercriminals are also exploiting its capabilities. This malicious use of AI presents new challenges for organizations. Threat actors are now leveraging AI to accelerate reconnaissance, improve attack success rates, and obfuscate their tracks. Whether it's phishing as a service or AI-powered social engineering, the threats are evolving faster than ever, making it imperative for defenders to stay ahead by leveraging AI themselves.

But the operational impact of AI extends beyond defense into the core processes of cybersecurity. AI isn't just helping defenders react faster; it's enabling them to proactively identify vulnerabilities and streamline operations. For example, AI is revolutionizing security operations centers by automating the analysis of user-reported phishing emails, reducing false positives, and identifying high-risk anomalies that would've otherwise been missed.

WHAT YOU NEED TO KNOW ABOUT AI-DRIVEN CYBERATTACKS!

There are multiple types of cyberattacks enables by AI and machine learning.

AI - POWERED CYBERATTACKS HAVE 5 MAIN CHARACTERSITICS!

- Attack automation: Until very recently, most cyberattacks required significant hands-on support from a human adversary. However, growing access to AI- and generative AI-enabled tools is allowing adversaries to automate attack research and execution.
- Efficient data gathering: The first phase of every cyberattack is reconnaissance. During this period, cyberattackers will search for targets, exploitable vulnerabilities, and assets that could be compromised. AI can automate or accelerate much of this legwork, enabling adversaries to drastically shorten the research phase and potentially improve the accuracy and completeness of their analysis.
- Customization: One of the key capabilities of AI is data scraping, which is when information from public sources — such as social media sites and corporate websites — is gathered and analyzed. In the context of a cyberattack, this information can be used to create hyper-personalized, relevant, and timely messages that serve as the foundation for phishing attacks and other attacks that leverage social engineering techniques.
- Employee targeting: Similar to attack customization, AI can be used to identify individuals within an organization that are high-value targets. These are people who may have access to sensitive data or broad system access, may appear to have lower technological aptitude, or have close relationships with other key target.

TYPES OF AI-POWERED CYBERATTACKS

AI-driven social engineering attacks leverage AI algorithms to assist in the research, creative concepting, or execution of a social engineering attack. A social engineering attack is any kind of cyberattack that aims to manipulate human behavior to fulfill a purpose, such as sharing sensitive data, transferring money or ownership of high-value items, or granting access to a system, application, database, or device.
In an AI-driven social engineering attack, an algorithm can be used to do the following:

- Identify an ideal target, including both the overall corporate target and a person within the organization who can serve as a gateway to the IT environment
- Develop a persona and corresponding online presence to carry out communication with the attack target
- Develop a realistic and plausible scenario that would generate attention
- Write personalized messages or create multimedia assets, such as audio recordings or video footage, to engage the target

AI-driven phishing attacks use generative AI to create highly personalized and realistic emails, SMS messages, phone communication, or social media outreach to achieve a desired result. In most cases, the goals of these attacks are the same as that of a social engineering attack: to access sensitive information, gain access to a system, receive funds, or prompt a user to install a malicious file on their device.
In advanced cases, AI can be used to automate the real-time communication used in phishing attacks. For example, AI-powered chatbots can support interactions that make them nearly indistinguishable from humans. Attackers can use these tools, deployed at scale, to attempt to connect with countless individuals simultaneously. In many cases, these chatbots pose as customer support or service agents in an attempt to gather personal information and account credentials, reset account passwords, or access a system or device.

A **deepfake** is an AI-generated video, image, or audio file that is meant to deceive people. Deepfakes commonly appear on the internet for no other purpose than to entertain and confuse. However, they can also be used more maliciously as part of disinformation campaigns, "fake news," smear campaigns of high-profile individuals, or cyberattacks.
In the context of a cyberattack, a deepfake is usually part of a social engineering campaign. For example, an attacker may use existing footage of a corporate leader or client to create a doctored voice recording or video footage. The tool can mimic the person's voice and instruct a person to take a specific action, such as transferring funds, changing a password, or granting system access.

AMERICA'S CYBER DEFENSE AGENCY (CISA)

In addition to offering a range of no-cost CISA-provided cybersecurity services, CISA has compiled a list of free services and tools provided by private and public sector organizations across the cyber community.
CISA has curated a database of free cybersecurity services and tools as part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments.

Visit : https://www.cisa.gov/ for more information and resources!

THE LATEST SCAMS YOU NEED TO BE AWARE OF IN 2025

Scammers often use new technology, such as AI, to enhance tried-and-true scams. Learn about the latest twists and types of attacks, and what you can do to stay safe in 2025.

Over the years, many scams have slowly evolved as scammers incorporate new technology and play off of the most recent major events. But there is a general sense that scams and fraud have become increasingly common around the world. The Global Anti-Scam Alliance (GASA) reports that over $1.03 trillion was lost to scammers in 2024.

Scammers almost always have the same goal—to get your personal information or money. Learning about the latest developments will hopefully help you stay one step ahead. The latest scams to watch out for in 2025 include AI-powered scams, imposter scams, sextortion scams targeting children and teens, romance scams, phone-related scams, cryptocurrency and investment scams, online purchase scams, employment scams, and check fraud.

While scammers' delivery methods and messaging can quickly change, a few basic security measures can help protect you from the latest and most common scams:

- Be skeptical when someone contacts you. Scammers can spoof calls and emails to make it look like they are coming from different sources, including government agencies, charities, banks and large companies. Don't share personal information, usernames, passwords or one-time codes that others can use to access your accounts or steal your identity.
- Don't click unknown links. Whether the link arrives in your email, a text or a direct message, never click on it unless you're certain the sender has good intentions. If the message says it's from a company or government agency, call the company using a number that you look up on your own to confirm its legitimacy.
- Be careful with your phone. Similarly, if you suspect a spam call, don't respond or press a button. The safest option is to hang up or ignore the call entirely. You can look up the organization and initiate a call if you're worried there may be an issue.
- Update your devices. Software updates may include important security measures that can help protect your phone, tablet or computer.
- Enable multifactor authentication. Add this feature to any accounts that offer it as an option, and try to use a non-SMS version to protect yourself from SIM swapping.
- Research companies before taking any actions. Before you make a purchase or donation, take a few minutes to review the company. Do a web search for its name plus "scam" or "reviews" and research charities on Charity Navigator and CharityWatch.
- Don't refund or forward overpayments. Be careful whenever a company or person asks you to refund or forward part of a payment. Often, the original payment will be fraudulent and taken back later.
- Look for suspicious payment requirements. Scammers often ask for payments via cash, wire transfer, money order, cryptocurrency or gift cards. These payments can be harder to track and cancel than other forms of payment, which can leave you stuck without recourse.
- Create a family password. Create a family password that you can all use to verify that it's really one of you on the phone, and not someone who created a deepfaked video or cloned voice.

To learn more, visit: https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware-of/