DTS DanTech Services
Computers under control!™

Technology Times September 2023 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Got IT Problems? - Click Here!

Social Engineering

By imperva

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

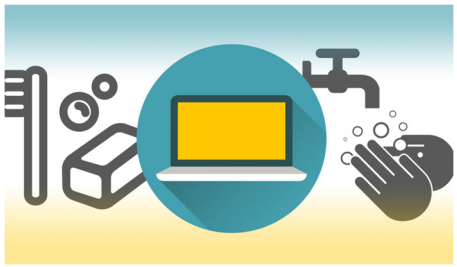
Social Engineering Attack Lifecycle
What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Social engineering attack techniques
Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Baiting
As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

- continued on Page 3

Cyber Hygiene



Being proactive means thinking ahead and preparing for worst-case situations. This is never more important than in your cybersecurity, due to the huge amounts of crucial data we have on our computers and the abundance of cybercrime and natural disasters.

While cybersecurity refers to the overall protection of a company's systems and data, cyber hygiene refers to the individual tasks that contribute to the cybersecurity of a computer.

Usually these tasks are the responsibility of an individual user, rather than that of an IT team.

Regular maintenance tips you should be doing to keep your computer safe:

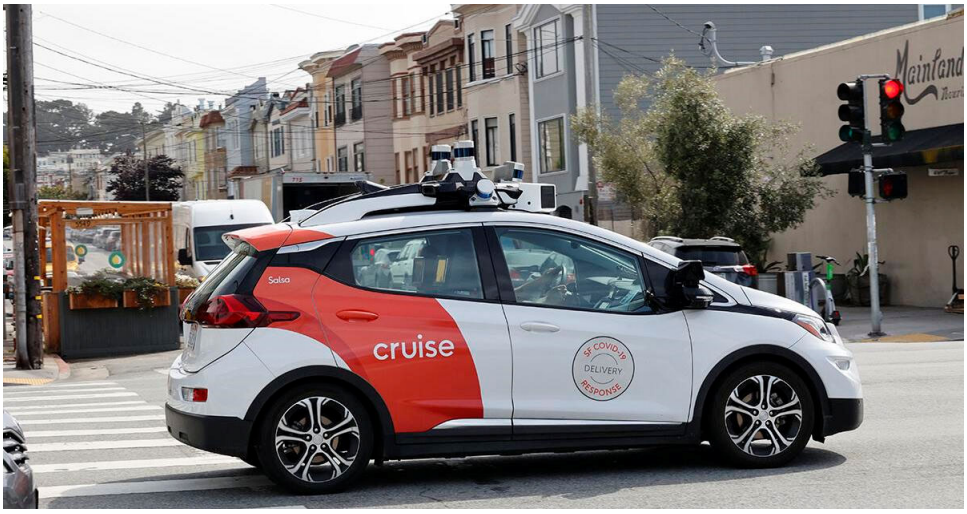
- Install anti-virus and malware software to scan for viruses
- Use firewalls to prevent unauthorized access to your network
- Strong passwords: Make passwords that are hard to guess; combinations of letters, numbers and symbols; and change them regularly
- Update apps, browsers, and software on all devices regularly
- Keep hard drives clean by reformatting and wiping them
- Use multi-factor authentication any time you can
- Back-up important files offline

Driverless Vehicles Produce Unfortunate Results in San Francisco

Self-driving taxis, or "robotaxis" were given the go-ahead to operate commercially 24/7 in San Francisco, in the middle of August. But the problems they caused, such as breaking traffic laws and endangering the public, indicate they're still not ready for the real world, some say.

The California Public Utilities Commission (CPUC) voted 3-1 in favor of allowing robotaxis to operate, and the proposal went ahead, despite much opposition from San Francisco officials and the public. The San Francisco Fire Department, for instance, had records of 55 incidents this year in which robotaxis interfered with their ability to fight fires and save lives by driving through yellow emergency tape, blocking firehouse driveways, and not moving out of the way of fire trucks. Yet still, the proposal was passed.

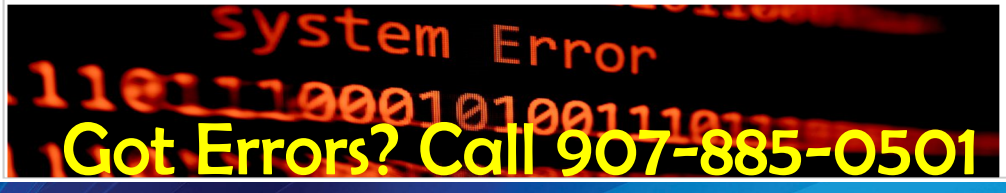
The chaos that followed the approval of the operation of robotaxis included a scene where ten Cruise vehicles -- stopped in place with hazard lights flashing -- blocked a road and intersection in the North Beach area.



Other incidents that occurred include multiple robotaxis illegally running stop signs and having to swerve to avoid pedestrians, which were posted on social media in August. In a less-dangerous and somewhat amusing case, another robotaxi was videoed driving into a construction and stopping in wet concrete.

San Francisco Board of Supervisors stated that the city will ask legislators to reconsider their decision to allow robotaxis to operate in the city for the sake of public safety, explaining that in the case of a power outage or natural disaster, these cars could potentially congest the streets at the crucial moment when emergency vehicles need to get into the city and the public needs to evacuate in a hurry.

It's unclear whether these driverless vehicles will continue to operate in San Francisco for the time being or the companies will pause the operation while they work to perfect this technology. Maybe this is all part of the growing pains that come with new and innovative technologies.



Shiny New Gadget Of The Month:

The Tap Strap 2 wearable keyboard

The Tap Strap 2 is a single handed all-in-one wearable keyboard, mouse & air gesture controller. Made out of Skin-safe TPU, Tap lets you control your devices for 10 hours on a full charge (7 days of standby)

- Keyboard Mode – Type letters, numbers, symbols and characters into your smart devices. Use any surface!
- AirMouse Mode – Input & control using Air Gestures into any Bluetooth device
- Optical Mouse Mode – Precise 1,000 DPI optical mouse enables on the go navigation, selection, scrolling, dragging and dropping in any environment using any surface.
- Controller Mode – Turn complex commands into simple finger taps and air gesture swipes to control your favorite apps, games and devices.

Custom Mode – your Tap Strap 2 is 100% customizable.

Use our free, simple & quick TapMapper web tool, open source SDKs, API's or Unity plugin to tailor your Taps to your needs.

"Social Engineering"
- continued from page 1

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list. Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware
Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected. Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Pretexting
Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task. The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data. All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.
Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

- continued on Page 4

Use PhotoGuard to protect your photos from AI manipulation

AI photo manipulation is very helpful when it comes to creative advertising, unblurring faces in family pictures, adjusting skin tone, or removing a photobomber with just the click of a button, but there are also malicious ways the technology can be used.

Cybercriminals are taking steps to broaden the use of AI. AI technology used for photo manipulation raises ethical concerns because of the risk of publishing misleading and deceptive content.

Right now, someone can take a photo and manipulate it to put us in bad-looking situations, leading to defamation or blackmail.

A research team of students and professors at MIT with the goal of protection against AI manipulation, introduced PhotoGuard – a technology that serves as a protective shield, disrupting AI's ability to manipulate an image. PhotoGuard works by using what the MIT research team refers to as "perturbations." These are minor alterations in select pixels, so miniscule they're invisible to the human eye yet detectable by computers.

These "perturbations" disrupt the AI's ability to read what the image is. If someone tries to use a photo editing software, such as Stable Diffusion, to manipulate an image that has been "immunized" by PhotoGuard, the result will appear unrealistic or warped.

"Social Engineering" - continued from page 3

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

Social engineering prevention

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

- **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.

- **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Use an easy-to-deploy 2FA solution that can increase account security for your applications.

- **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.

- **Keep your antivirus/antimalware software updated** – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.