UNICAL ACADEMY

4. TOP 6 SOCIAL ENGINEERING THREAT PREVENTION TRENDS IN 2020

Top 6 Social Engineering Threat Prevention Trends in 2020:

Social engineers operate at a psychological level, where they manipulate human feelings, such as curiosity, anger, or fear, to work out schemes and draw victims into their planned traps.

Therefore, users need to be aware and alert whenever they feel alarmed by a suspicious email, get inclined to an offer on a website, or come across stray digital media undertaking unknown sensitive activity such as collecting account credentials.

Being alert and aware can help users protect themselves against most social engineering attacks in the digital realm. Here are the top six social engineering threat prevention trends in 2020.

01.

Safe communication and account management habits:

An individual is vulnerable to external threats only when he is exposed to some form of online communication or interaction – such interaction includes communication on social media, email, text messages, and in-person interactions. Following best practices can act as a firewall against social engineering attacks.

Do not click on links in emails or messages.

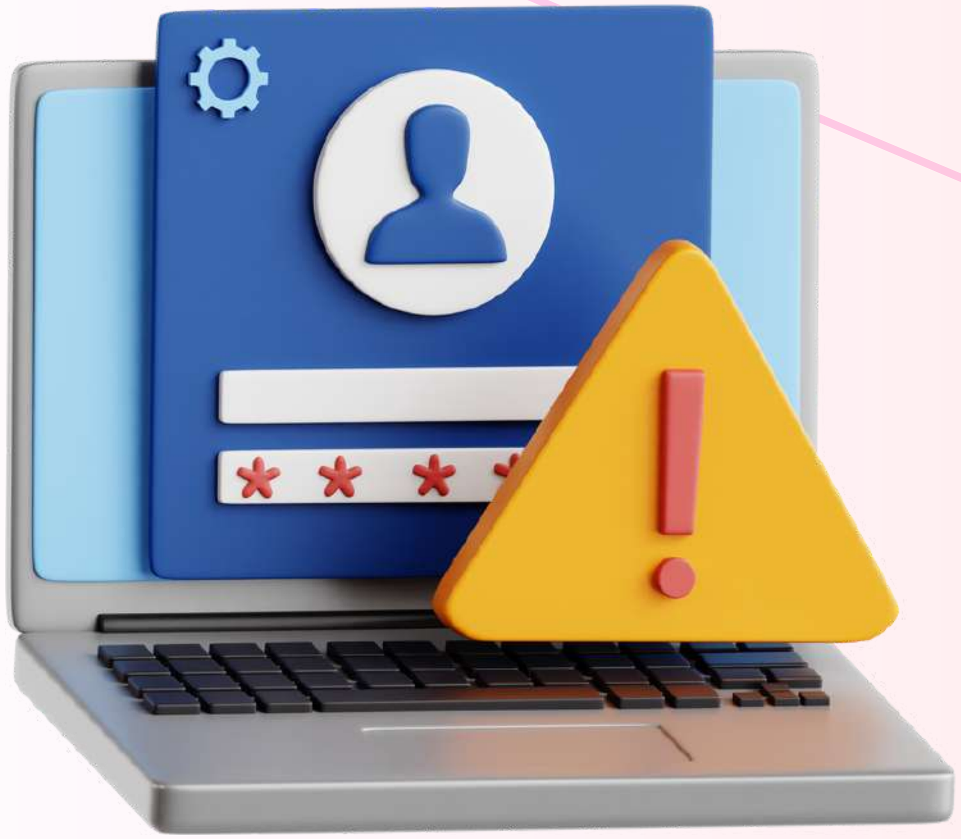
Always manually type a URL into the address bar, regardless of the sender. Also, take extra precaution in investigating to identify an official version of the URL under consideration. Do not engage with any URL that is not verified by you as official or is legitimate. Further, do not open attachments from suspicious sources.

Use multi-factor authentication.

The safety of online accounts is ensured when the user uses more than just a password to protect them. Multi-factor authentication adds additional layers to verify the user’s identity upon login. Such factors can include user biometrics data like a fingerprint or facial recognition, or OTP passcodes sent via text message.

Use strong passwords.

Each user's password should be unique and complex, implying that the password should be difficult to guess. Try using various character types, such as uppercase, lowercase, numbers, and symbols. Further, prefer opting for long passwords.



Avoid sharing personal details.

Do not unknowingly expose answers to security questions or parts of a password while interacting with anything or anyone. Try setting up security questions that are memorable but inaccurate. By doing so, you'll make it harder for a criminal to crack the target account.

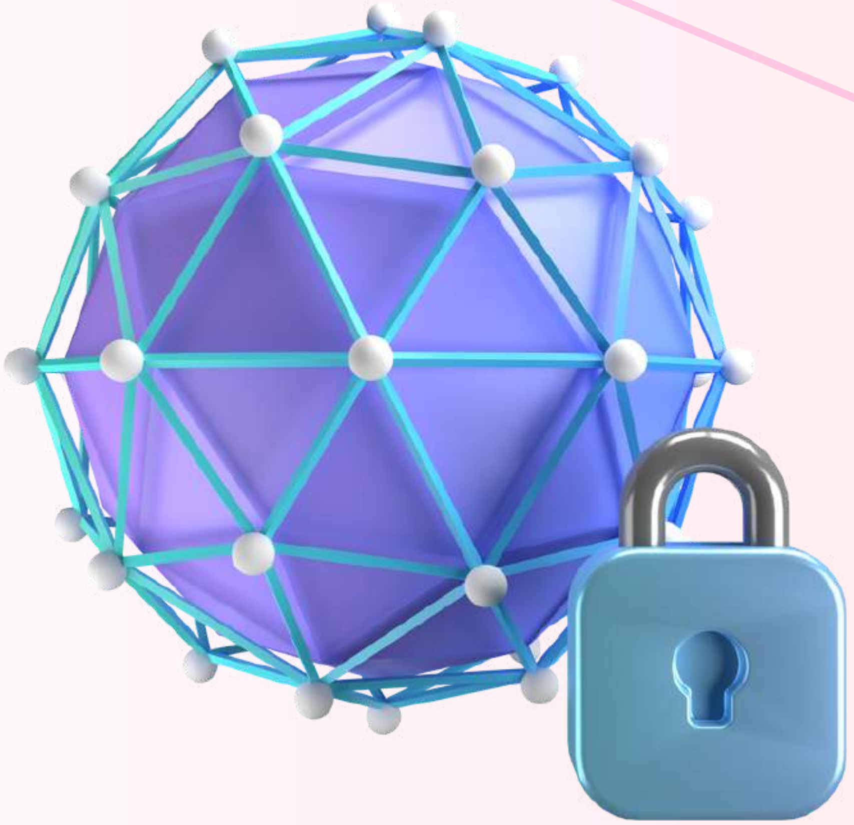
Cautious online friendships.

Although the internet is a great way to connect with people worldwide, it is also a common platform for social engineering attacks to flourish. So, watch out for red flags that indicate psychological manipulation or a clear abuse of trust.

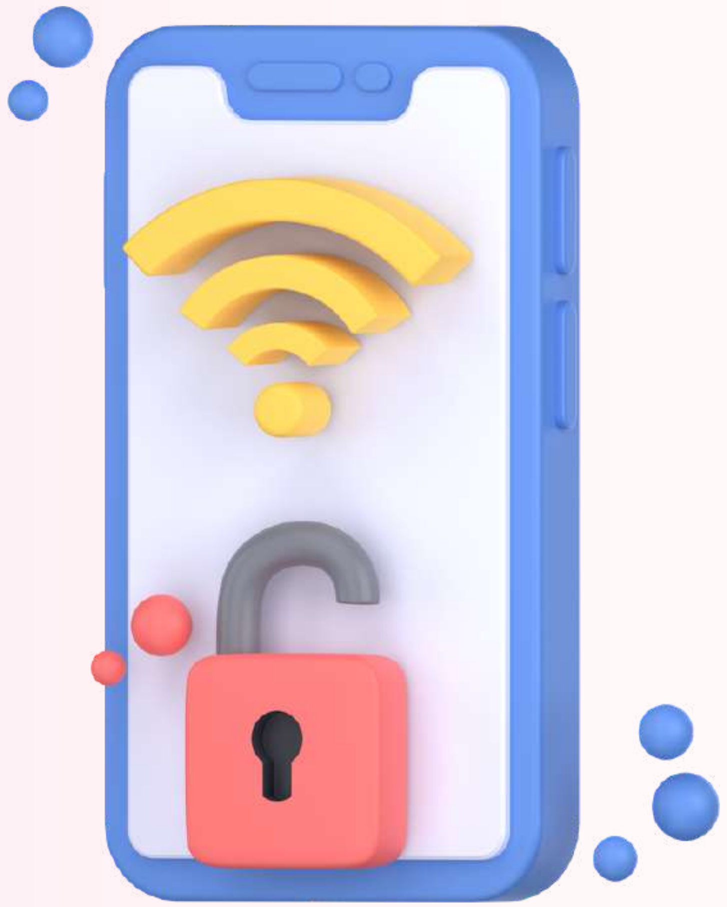
02.

Safe network use habits

Vulnerability can be exploited to its maximum stretch in compromised online networks. Hence, to safeguard users' data from getting tampered with and misused during social engineering attacks, it is important to take protective measures for any network that the user is connected to.



Do not allow strangers to connect to your primary Wi-Fi network.



Strangers at home or in the workplace should be allowed to access Wi-Fi via a guest Wi-Fi connection. Such an arrangement allows the main encrypted, password-secured connection to stay secure and interception-free. If any third party tries to “eavesdrop” for information, they won’t be able to access the activity you and others have kept private.

Use a VPN.

In scenarios where someone on the main wireless network (or wired, or cellular) finds a way to intercept traffic, a virtual private network (VPN) can keep such intruders out.

VPNs provide services that allow users to keep their internet connection private over an encrypted “tunnel”. The connection is safeguarded against third-party intruders and eavesdroppers. Users’ data is anonymized so that it cannot be traced back to the user via cookies or other means.

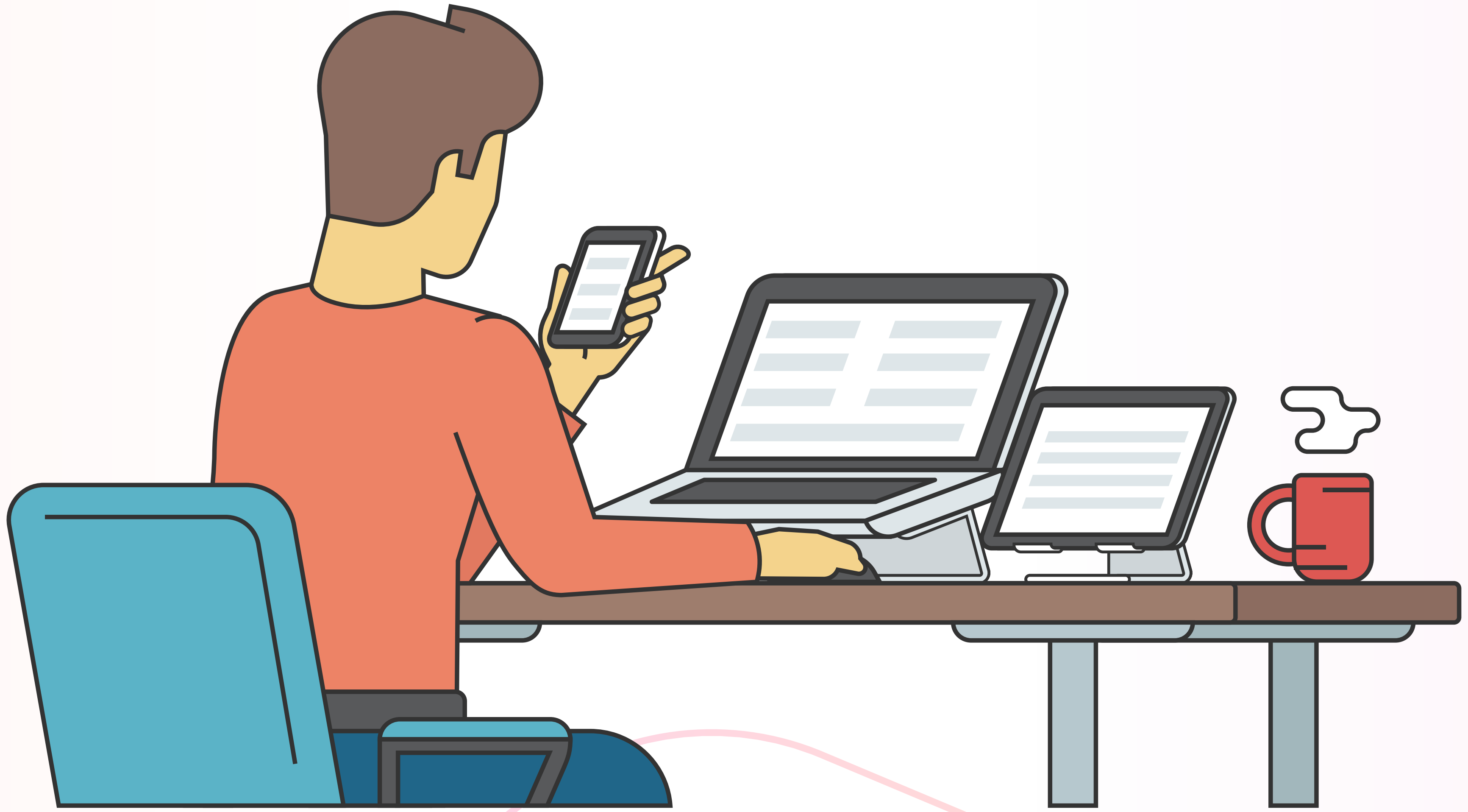
Security of network-connected devices and services.

Securing network-connected devices, smart devices, and the cloud services associated with these devices is important. Protect the generally overlooked devices, such as home network routers or car infotainment systems, home theatres, etc. Data breaches on all these devices could spark personalization for a potential social engineering scam.

03.

Safe device usage habits

Keeping devices safe is just as important as managing digital behaviors. Mobile phones, tablets, and other computing devices can be protected by following the below tips:



Comprehensive internet security software.

In scenarios when social attacks become successful, malware infections are a general outcome. To fight the rootkits, Trojans, and other embedded bots, it’s important to employ a sophisticated internet security solution to eliminate infectious intrusions and track their source.

Do not leave devices unsecured in public.

The best practice for a user at a workplace or any public setting is to always lock the computer and mobile devices so that no one gets ready access to these devices. In public places like airports, cafes, or commercial markets, always keep these devices in your possession.

Keep all your software updated.

Patch updates give software essential security fixes. As the updates are delayed or skipped, the software unknowingly exposes security holes for attackers to target. As criminals are generally aware of the characteristics of most computers and mobile users, you become a vulnerable target for socially engineered malware attacks.

Check for known data breaches of your online accounts.

Actively monitor new and existing data breaches for your online accounts, such as email addresses. Use security cloud services Opens a new window that provide a notification when the user’s online account data is compromised. These cloud services further advise on taking action against data breaches.

04.

Security awareness training

Healthy cybersecurity is aligned with human behavior. Social engineering dictates attacks by manipulating psychological behavior. Consider a phishing email, wherein the recipients are encouraged to click on an embedded link within the email or download a malicious file.

Cybercriminals make the emails look like an authentic entity by using traits such as trust and a sense of urgency to disguise the nefarious email. Thus, ensuring that the entire workforce understands the various tricks followed by cybercriminals can be the best defense against social engineering.

Social engineering protection begins by creating the right kind of awareness among individuals by educating them. If all the users are educated and alerted about such social assaults from time to time, then the collective safety of the society can be enhanced many folds.

Hence, sharing the learned knowledge of these risks with co-workers, friends, and family can increase awareness among the masses, thereby allowing better remediation against any kind of social engineering attack.

05.

Regular cybersecurity posture assessments

With each attack, cybercriminals tend to update and modify the social engineering techniques that they use to attack an environment. As deepfakes technology emerges in the security landscape – that manifests AI techniques for manipulating a voice or face, the social engineering attack techniques may also change.

Hence, advancing the cybersecurity posture assessment to help organizations strengthen their cybersecurity defenses by developing a comprehensive cybersecurity roadmap is of paramount importance.

Cybersecurity posture assessment represents an insightful and useful first step for organizations looking to identify their current position in terms of security, currently missing components, and what needs to be done to increase their cybersecurity maturity level.

06.

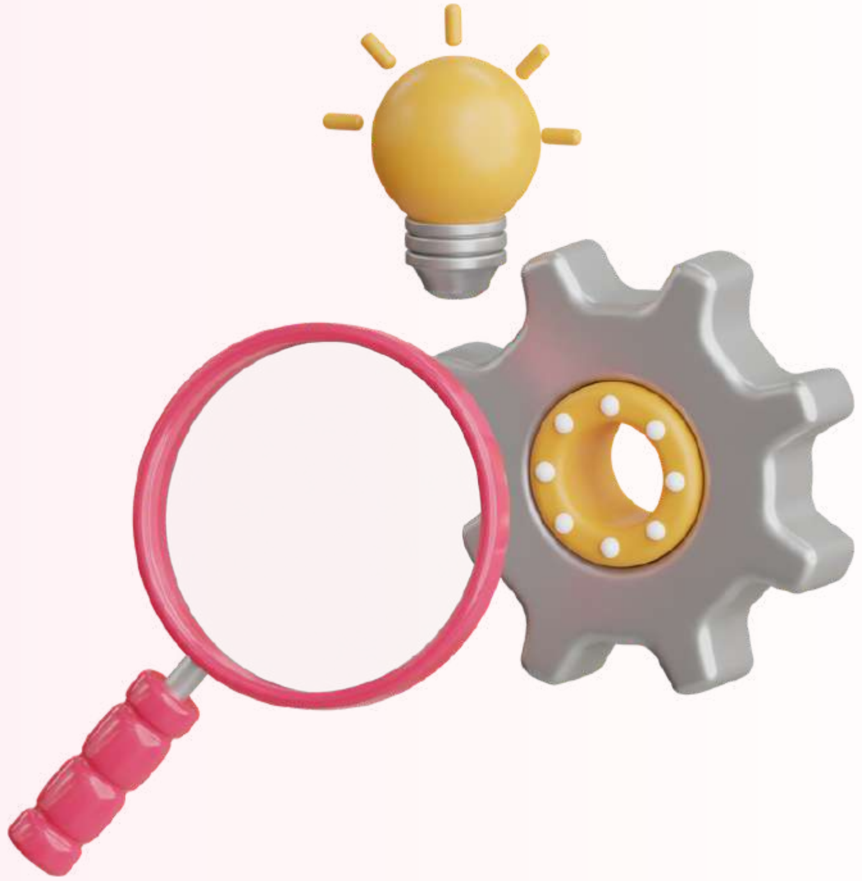
24/7 monitoring practice

The security team's vigilance can be enhanced by testing and validating services that provide 24/7 monitoring.

Businesses need to find a way to monitor their environments 24/7 cost-effectively if they wish to comply with regulations, secure their environment against cyberattacks or data breaches, or guarantee upward operational uptime.

UNICAL ACADEMY

Monitoring involves using tools that can help detect problems on the network in real-time. Such tools may include techniques for performing behavioral analysis and some smart tools that may help to spot anomalies.



Therefore, monitoring enhances the system’s overall security by ensuring that software is kept up to date during all times and misconfigurations of servers are duly addressed.