

BY ISHAAN SHARMA AND KARTIK VEDI



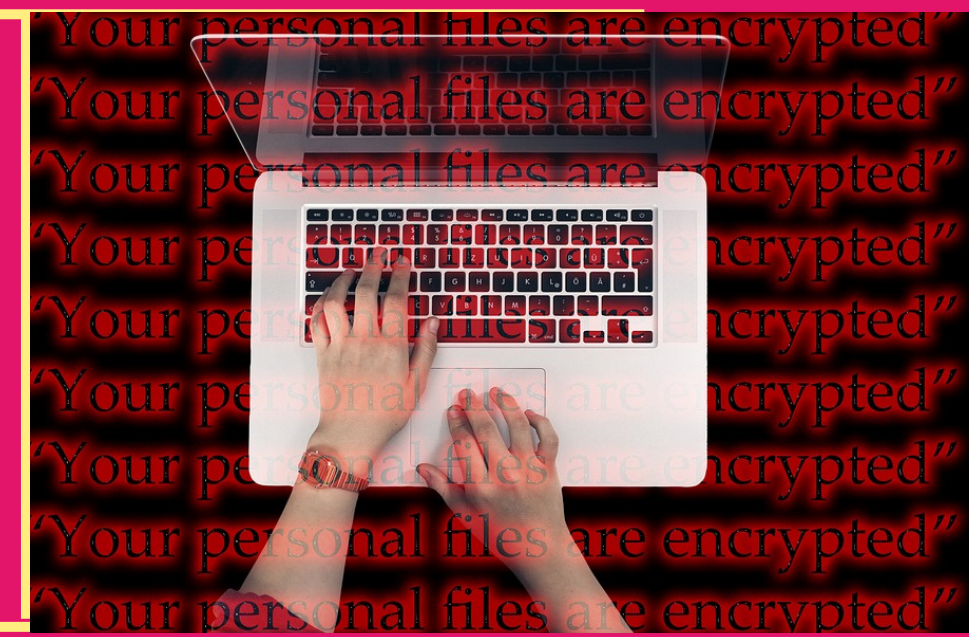
Operating systems often have built-in defenses against keyloggers, but users should also be cautious and avoid suspicious links or downloads. Keyloggers are software or hardware that record every keystroke made on a computer or device. While they can be used for legitimate purposes, they can also be used maliciously to steal sensitive information such as passwords.



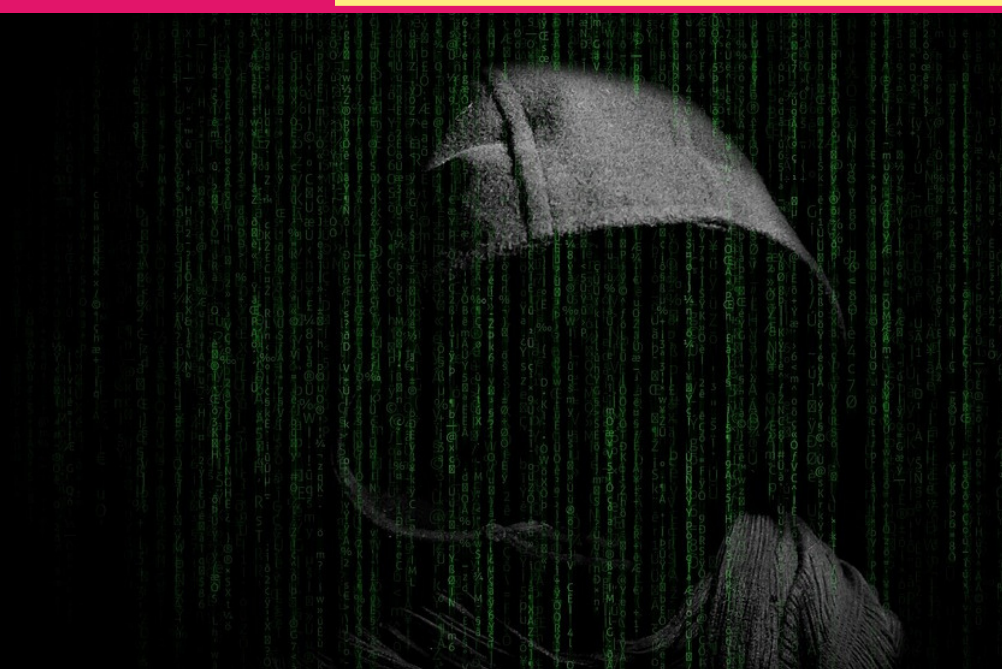
Employing passwords is crucial in ensuring the confidentiality and security of personal and sensitive information in digital environments. The use of strong, unique passwords can prevent unauthorized access and protect against potential data breaches. The use of strong, unique passwords can enhance the security of operating systems and prevent malicious activities such as hacking, data theft, and identity fraud.



Being cautious while clicking on links is crucial in preventing various cyber threats, including phishing scams and malware infections. It is important to avoid clicking on suspicious links or those from unknown sources to maintain the security and integrity of personal and sensitive information.



It is crucial to refrain from using passwords in public places when accessing smartphones to maintain the security of personal and sensitive information. Public use of passwords can increase the risk of unauthorized access and compromise the integrity of digital assets, highlighting the importance of taking precautions while using smartphones in public.



It is important to avoid using unauthorized sources when upgrading operating systems to ensure the security and integrity of digital devices. The use of unofficial sources for such upgrades can pose significant risks, including malware infections and other forms of cyber attacks. Therefore, it is crucial to only use legitimate sources when upgrading operating systems to maintain the safety of personal and sensitive information.

