ESSENTIAL PRACTICES FOR PERSONAL SECURITY

26 Dec, 2023 Volume 2 Issue 7 2 views

By Zul Karami Che Musa , Mahathir Muhamad , Abd Aziz Mat Hassan , Muhammad Naqib Mat Yunoh & Dr. Mohd Zulkifli Muhammad

In today's interconnected digital landscape, safeguarding personal information has become more crucial than ever. Cyber threats loom large, ranging from sophisticated phishing techniques to malware attacks, constantly evolving and targeting unsuspecting individuals.

To navigate this landscape securely, adopting proactive measures and adhering to robust cybersecurity practices are imperative. Understanding and implementing foundational strategies can significantly bolster personal defenses against these ever-present risks. Here are some essential practices for your personal security.

Update Cybersecurity Knowledge and Understand Scammers' Modus Operandi

Staying informed about evolving cyber threats is pivotal. Scammers often employ sophisticated tactics, including phishing, social engineering, and malware distribution. Familiarizing yourself with their methods enhances your ability to spot and thwart potential attacks. Awareness of scams prepares individuals for potential attempts at manipulation or coercion. Knowing how scammers operate can make people more psychologically resilient and less susceptible to emotional tactics employed by fraudsters.

Use Strong Passwords, Multi-Factor Authentication and Password Managers

Adding layers of security, such as multi-factor authentication, significantly bolsters defense against unauthorized access. Employing strong, unique passwords, or utilizing a password manager, enhances protection against brute-force attacks. Under no circumstances should you share your password or one-time password with anyone, including close friends or relatives, as they could potentially exp' spoofing techniques.

latest threats and reduce the risk of exploitation by malicious actors.

Avoid Accessing Personal or Financial Data via Public Wi-Fi

While public Wi-Fi networks provide convenience for staying connected on the go, there are potential risks associated with their use. The lack of encryption and security measures on these networks makes it easier for hackers to intercept data transmitted between your device and the network. Cybercriminals may exploit public Wi-Fi to conduct man-in-the-middle attacks, where they intercept and potentially alter the communication between your device and the internet. This can lead to unauthorized access to sensitive information.

Disable Unnecessary Features (GPS, Bluetooth)

Keeping GPS and Bluetooth on when not in use can potentially expose your device to security vulnerabilities. Cyber attackers may exploit these features to track your location, gather information, or attempt unauthorized access to your device. Bluetooth, when left on, can be susceptible to certain attacks, such as Bluejacking or Bluesnarfing. Turning off Bluetooth when not in use reduces the chances of unauthorized access or data theft through Bluetooth vulnerabilities.

Choose Apps Wisely

There are several reasons why you should exercise caution and avoid installing APKs (Android Application Package files) from untrusted sources. APK files obtained from unofficial sources may be modified or tampered with, introducing security vulnerabilities or malicious code. Installing such files can compromise the security of your device and personal data. Therefore, you should prioritize downloading applications from reputable sources like official app stores, and review app permissions before installation to ensure they align with their intended functionality.

Be Skeptical About Links and Attachments

Links in emails, messages, or social media posts may lead to phishing websites that mimic legitimate sites to trick you into providing sensitive information such as login credentials, personal details, or financial information. Clicking on malicious links or opening suspicious attachments can result in the download and installation of malware on your device. Malware can compromise your system security, steal data, or perform other malicious activities.

Do not allow strangers to borrow your phone

Some strangers may exploit the opportunity to use your phone for malicious purposes, such as making unauthorized calls, sending harmful messages or engaging in activities that could have legal consequences for you. Simply connecting your mobile phone to a device has the potential to install harmful applications or malware.

Security Scammers Privacy Technology

Become the first to comment

Related posts

PENDAPAT

"JUTAWAN SEGERA" PUNCA KECENDERUNGAN BELAJAR ANAK MUDA PUDAR

26 Dec, 2023 Volume 2 Issue 7 17 views

Sejak pandemik Covid-19 melanda negara pada tahun 2020 dan 2021, tidak dapat dinafikan semakin ramai anak muda yang bekerja keras mencari nafkah untuk kelangsungan hidup dan memperbaiki taraf kehidupan mereka.

PENDAPAT

UNRAVELLING TRUST: PSYCHOLOGICAL CONCEPTS BEHIND WHY PEOPLE FALL FOR SCAMS

26 Dec, 2023 Volume 2 Issue 7 22 views

Scams are becoming more common and sophisticated in the digital age, which puts people and societies at serious risk. Even with increased awareness and warning statements, scammers still manage to swindle individuals. In order to create tactics to stop these dishonest activities, it is essential to comprehend the psychological and social concepts that explain why individuals fall for scammers.

PENDAPAT

UNLEASHING THE POWER OF DIGITAL TECHNOLOGIES IN ECONOMICS

25 Oct, 2023 Volume 2 Issue 6 75 views

The widespread impact of digital technologies has caused a profound change in how our world operates in the twenty-first century. The symbiotic relationship that these technologies have with the economy has grown more and more entwined, changing the fundamental nature of contemporary economic activity.

Follow us

Twitter

Instagram

Pinterest

Categories

Pendapat	(69)
Hasil Kajian	(20)
Berita	(5)
Kreatif	(3)

Lastest Post

PENDAPAT

KEUSAHAWANAN WANITA: PROSPEK DAN CABARAN MASA HADAPAN

26 Jan, 2023 428 views

PENDAPAT

EXPLORING THE ROLE OF MALAYSIAN PARENTS IN NATIONAL SPORTS TALENT MANAGEMENT

10 May, 2023 63 views

PENDAPAT

EKONOMI DIGITAL DAN USAHAWAN

26 Feb, 2023 776 views

PENDAPAT

STUDENTS' ATTITUDES AND THEIR POTENTIAL FOR SUCCESS

27 Sep, 2023 273 views

PENDAPAT

KELESTARIAN PENGURUSAN KEWANGAN MENDORONG KEJAYAAN USAHAWAN

26 Feb, 2023 675 views

PENDAPAT

ESSENTIAL PRACTICES FOR PERSONAL SECURITY

10 Jan, 2024 2 views

Tags

Usahawan Prediction Twitter Pendapat Covid-19 Kesihatan Fizikal Poisson Process Platform Technology Popularity

Recently Viewed Posts

PENDAPAT

UNRAVELLING TRUST: PSYCHOLOGICAL CONCEPTS BEHIND WHY PEOPLE FALL FOR SCAMS

03 Jan, 2024 22 views

About us

Caknawan menjadi platform kepada penulisan popular ilmiah hasil sumbangan artikel-artikel daripada pensyarah-pensyarah institusi pengajian tinggi di Malaysia.

Address
Fakulti Keusahawanan dan Perniagaan, Kampus Kota, Pengkalan Chepa, 16100 Kota Bharu, Kelantan

Phone
+6097717127

Popular Posts

EKONOMI GIG DI MALAYSIA : PROSPEK DAN CABARAN
26 Jan, 2023 3,484

TREND MEDIA SOSIAL: PELUANG PENTING BAGI PERNIAGAAN UNTUK BERKEMBANG MAJU
29 Sep, 2022 1,932

KETAGIHAN PERMAINAN DALAM TALIAN
01 Sep, 2022 1,497

Quick links

Homepage Contact
Blog About

Tags

Usahawan Prediction Twitter Pendapat Covid-19

Newsletter

Subscribe to Our Newsletter