Electronic Communications Coordinator   George Michael & Maria Efthymiou

Goals

The Region 8 Electronic Communication Coordinator's job is to facilitate communication, both between members of the Region 8 Committee and between this committee and present or future IEEE members.

What is involved:

1. Supporting technically and administratively the committee meetings.
2. Performing content updates to our web server.
3. Managing access rights to the various systems we administrate.
4. Performing security and other feature updates to our web server.
5. Maintaining and updating our mailing distribution lists.
6. Creating new OU's websites at our web server and supporting their initial steps.
7. Supporting the chairs and appointed members during online meetings.
8. Creating custom pages at our website to perform custom functionalities.
9. Performing bug fixes caused by updates to our web server.
10. Investigating new technologies.
11. Developing tools as needed (e.g., the on-screen timer adopted by IEEE and is used at the board of directors; it was developed by us by our own initiative).
12. Investigate Cybersecurity issues.

Progress against goals since the last report

Website statistics from JetPack:
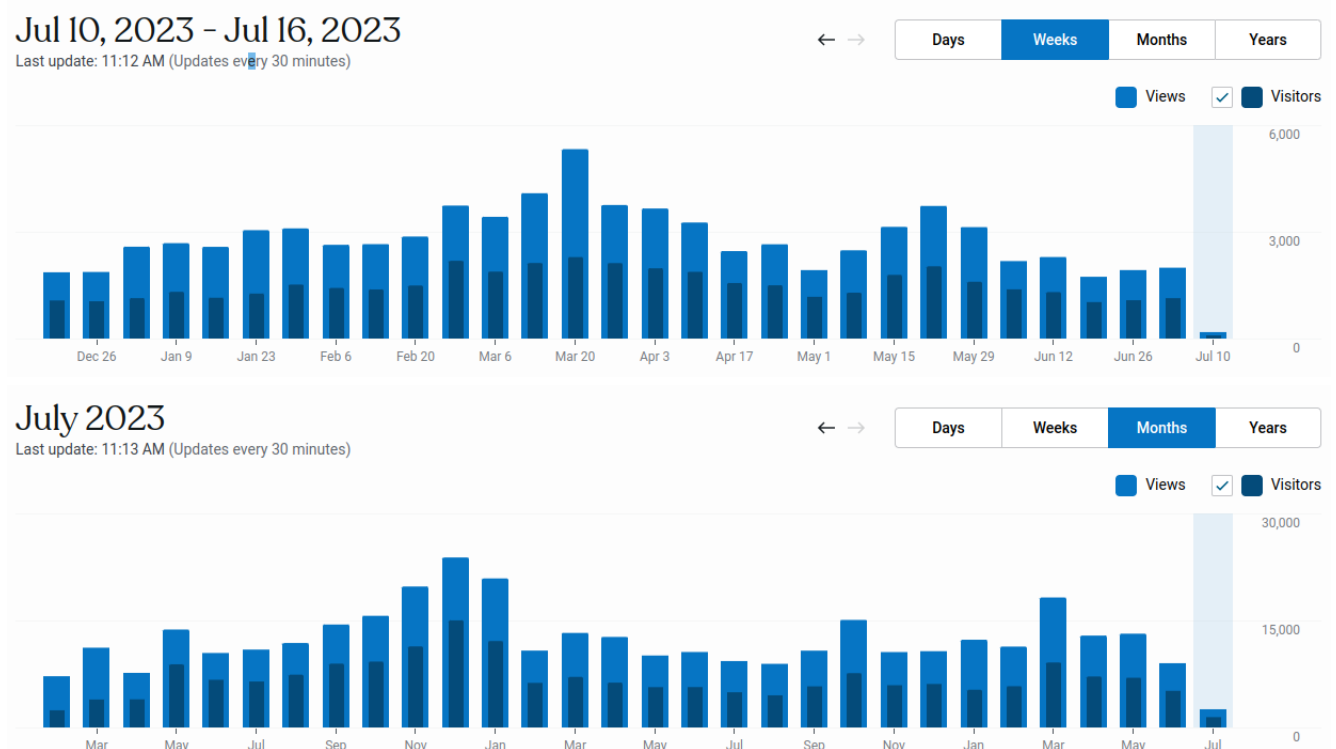
Deletion of stale websites and cleanup of DNS

To make sure our platforms are easy to maintain and secure, we recently cleaned up old websites and removed unnecessary DNS entries. By getting rid of outdated websites, we made our online space more organized and user-friendly. This also makes it easier for us to manage and update our digital resources. Additionally, we cleared out unused or unauthorized DNS entries, which helps protect our platforms from potential security threats. These actions were important for keeping our platforms strong and reliable, ensuring that our online presence is safe and trustworthy.

IEEE NextGen

Just like the previously identified vulnerability in "OU Analytics" that exposes critical volunteer information to all registered members, we have discovered a comparable issue in "IEEE NextGen." We are currently in the process of preparing a report detailing this second problem. It is important to note that the vulnerability in "OU Analytics" remains unaddressed, despite our previous identification.

It is crucial to address and fix these problems for several reasons:

1. Data Privacy and Security: Both "OU Analytics" and "IEEE NextGen" vulnerabilities compromise the privacy and security of sensitive information. This includes exposing critical volunteer details, which could potentially be misused or accessed by unauthorized individuals. By fixing these problems, the organization can ensure that the personal data of their members and volunteers is protected and that privacy breaches are minimized.

2. Trust and Reputation: Failing to address such vulnerabilities can severely impact the trust and reputation of the organization. Members and volunteers rely on these platforms to handle their data securely, and any indication of negligence in protecting their information can lead to a loss of trust. By actively fixing these problems, the organization can demonstrate their commitment to data protection and reinforce trust among their user base.

3. Compliance with Regulations: Data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, impose legal obligations on organizations to safeguard personal information. Failure to comply with these regulations can result in significant financial penalties and legal consequences. By addressing the identified vulnerabilities, organizations can ensure compliance with relevant regulations and mitigate the risks associated with non-compliance.

4. Mitigating Potential Harm: The identified vulnerabilities have the potential to cause harm to individuals whose information is exposed. This could range from identity theft and fraud to reputational damage or harassment. By fixing these problems, organizations can prevent or minimize the potential harm that could be inflicted upon their members and volunteers.

5. Continuous Improvement: Addressing vulnerabilities and actively working to fix them is a part of a broader commitment to ongoing improvement and security. By proactively identifying and resolving issues, organizations can enhance their systems, processes, and practices, making them more resilient against future threats. This proactive approach promotes a culture of continuous improvement and ensures that data security remains a priority.

In summary, it is important to fix these problems to protect data privacy, maintain trust, comply with regulations, mitigate harm, and foster a culture of continuous improvement in data security.

Website and Mailing Lists

The Region 8 website and mailing lists have been updated to reflect the current structure of the R8 committee. These updates ensure accurate information, transparency, and improved engagement. However, please note that certain changes are still pending approval before implementation.

New IEEE R8 SAC website

We have started working on the new IEEE R8 Student Activities Committee website. Currently, we are waiting for IEEE hosting provider to respond and discuss the specific details that will make this website different from other IEEE sites. We also have access to a library of plugins and tools that will help us develop the new site more effectively. These resources will enable us to create a user-friendly and feature-rich website for the committee. Our goal is to support IEEE R8 SAC build an innovative and visually appealing platform that showcases the committee's activities and provides a great online experience for users.