For Janet, network security and stability are key priorities. But both are under constant threat, and sometimes, lives can be at stake, too. The Computer Security and Incident Response Team (CSIRT) is the gatekeeper that keeps Janet safe.

The team’s brief is simple: to preserve the confidentiality, integrity, and availability of the network and everything on it, but the challenges are increasingly complex. CSIRT defends the Janet network against thousands of attacks every year. These take many forms: from coordinated attacks by botnets, to aggressive denial of service attacks, and malware distributed by criminals.

Beyond safeguarding the network, CSIRT also advises the community on security issues – sharing details of the latest threat, assisting customers with recovery following a compromise and coordinating information across the community. The team’s mission is to create a secure online working environment for the research and education community.

Enterprising software

A network of Janet’s size and complexity can’t easily or cost effectively be protected by any single, off-the-shelf security product. Instead, Janet builds them in-house from open source tools, drawing on the expertise of the team to develop a service best suited to our customers. Janet serves as many as 18 million end users, using 100Gbit/s links – well beyond the reach of most enterprise-level software.

CSIRT’s work breaks down into monitoring, responding and reviewing. While customers send in details of incidents via email, Janet CSIRT uses Netflow-based anomaly detection to spot suspicious activity on the network. Netflow provides information that is the equivalent of an itemised phone bill – the team can’t view the content of communication, but they can proactively detect known malicious activity, due to the real-time analysis of the data.
Netflow also supports the team’s forensic post-incident analysis, providing information as to what happened and what steps need to be taken to contain and resolve each incident.

Many attackers – one defender
Janet CSIRT deals with a number of incidents, ranging from a virus to a sophisticated and targeted attack by a hacker. Since the network also carries sensitive research data we’re also aware that there is potential for certain organisations to be targets for espionage. These incidents can be picked up by in-house systems or reported to us by our community.

But there are also bigger issues at stake – Janet’s user profile is different to other networks. Many users are children and vulnerable adults and CSIRT frequently liaises with the police through the Child Exploitation and Online Protection Centre (CEOP) to protect their safety. An extreme example of this type of incident is someone expressing suicidal thoughts on an Internet chatroom – Janet is able to respond to requests by the CEOP to locate the user, thus preventing a worst-case scenario. These types of incidents are a big priority for CSIRT.

The team is also on hand to discuss issues that are less life-and-death than the above example, but still a priority for Janet and our community. Incidents that are considered harmless can still help us to track trends and build up a picture of activity on the network – potentially preventing a more serious incident in the future.

Get in touch
Janet CSIRT’s priority is to keep our customers’ information systems working, so we welcome open dialogue with the community, sharing best practices to avoid malicious attacks compromising networks, and also educating users on how to tackle low-level cybercrime. Incidents can impact more than one site or organisation, so the team quickly shares information about new vulnerabilities with other Janet customers.

The most important weapon in CSIRT’s arsenal is information. Whether it comes from monitoring, or users reporting problems, it’s the key to keeping Janet and our community secure online. Mutual trust also plays a vital role in keeping the network safe – we depend on users reporting incidents on their own networks, and our community depends on the discretion and professionalism of our security experts. Every incident has the potential to affect others, so everyone on the network is responsible for security.

Effective networking
The explosion in use of mobile devices has created another issue for the team. Anyone can access the network from any device and every access point to the network is potentially another vulnerability, so Janet ensures it continues to match evolving technology.

Information from Janet’s users keeps the network safe, so Janet shares intelligence, technology and skills with other European research and education CSIRTs, security groups and law enforcement agencies. These communication channels are kept open so they work smoothly and effectively when they are needed. Members from Janet CSIRT speak at events and use social media, particularly Twitter, to keep up to speed with events in the information security community.

But whatever the medium the message is the same: when in doubt, report it.

The team are at their desks from 0800–1800 Monday to Friday. Out of office hours, they also manage a helpline 0300 999 2340 and remain on call until midnight during the week. The network is monitored 24/7.