What are phishing attacks?
Phishing attacks are cyber-attacks designed to deceive internet end users to steal personal information. Users are lured to websites that mimic the real site and are prompted to enter personal information. These sites are called phishing sites. There are three types of countermeasures for phishing sites.

User education
Provide users with knowledge to distinguish phishing sites using URLs, domains, and EV SSL certificates.

Interface improvement
Improve interfaces allowing users to easily distinguish safe and dangerous websites.

Detection of phishing sites
Compare phishing site URLs by pattern matching and calculate likeliness of phishing sites to alert users so they can make informed decisions.

Phishing countermeasures using eye-tracking
In 2013-14, NECOMA investigated where on the browser end users were looking when faced with a phishing site. Users skilled at detecting phishing sites look at URLs and SSL certificates (figure below, blue dots), while those not as skilled view the content of the site not in the address bar (red dots).

However, because phishing sites closely resemble the site, distinguishing the two on content alone is difficult.

Damage due to phishing
In 2013, phishing attacks caused an estimated 700 billion yen of damage worldwide. Over 10,000 phishing sites were reported monthly in 2014, indicating an increase in the scale of threats.

EV SSL certificates
After rigorous screening, an SSL certificate is issued. Current and commonly used browsers make users aware of the safety of the site by changing the color of the address bar to green when accessing sites using EV SSL certificates.

The Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis (NECOMA) project develops technologies to protect users from cyber threats.

As countermeasures against phishing attacks on users, we are implementing applications to promote proper habits of browsing when authenticating websites.

Besides R&D on optimal countermeasures against cyber threats based on user skill and browsing environments, we are developing international standardization.
Development of phishing countermeasure technologies using eye-tracking devices

Countermeasures using eye-tracking: EyeBit
To reduce the risk of phishing sites stealing personal information and to create the habit of automatically confirming URLs and SSL certificates, EyeBit trains users to check the address bar. EyeBit, which tracks eye movements, is a browser extension that requires users to look at the address bar prior to entering information in form fields. Below are screenshots before (left) and after (right) looking at the address bar.

The NECOMA Project has three primary pillars to popularize EyeBit technology: education, international standardization, and open sourcing.

Education
Classes on phishing countermeasures, which include an explanation of the results at NECOMA, are held at higher educational institutions worldwide. In 2015, classes were given to primary school students.

International standardization
We participated in SG17 held by ITU-T, an international standardization organization. We proposed recommendations in the field of cyber security and promoted R&D in this field.

Open Sourcing
EyeBit is available as open source software. Both commercial and non-commercial uses are possible. ※Download link https://github.com/necoma/

Phishing prevention by eye-movement analysis
The NECOMA Project is developing technologies to prevent users from being deceived by phishing sites. This technology, which measures and analyzes eye-movements, is based on the latest research in cognitive psychology as well as the duration and frequency with which a user looks at the address bar or security information and can distinguish between “blank stares” and “meaningful stares.” This information is used to analyze user intent towards website authentication.

Application to smartphone users
Due to the small size of the display on smartphone screens, security information can be inadequately presented. Using a small tablet device, we evaluated the cyber prevention technologies developed by the NECOMA Project to improve safety without reducing user convenience.

Development of future security technologies
Attacks targeting users rather than computer systems, have been increasing. To protect users, researchers of the NECOMA Project believe it is necessary to understand what users are thinking, and have focused on eye-tracking analysis and cognitive psychology. We will continue developing technologies to counteract various cyber-threats using various type of biological information.

Eye-tracking devices
Eye-tracking devices measure the direction of eye movement in humans. Measurement methods include the corneal reflection method, the EOG method, etc.

Cognitive psychology
This interdisciplinary field analyzes human mental states through measurable information. NECOMA uses eye-movement information to develop technologies that predict the intent of end users browsing websites.

EyeBit documentation
An easy-to-understand explanation on EyeBit can be found on our blog, and a detailed technical explanation can be found in our publication, both of which are available on the NECOMA Project website.

Please see http://www.necoma-project.jp for details on research activities and results of NECOMA.