Fraudulent mass-messages (phishing emails) being sent out to external email addresses from a cracked PC of the University of Electro-Communications

June 3, 2016

Chief Information Security Officer (CISO)
of the University of Electro-Communications
Wataru MITSUHASHI

The University of Electro-Communications (hereinafter referred to as UEC) (President: Takashi FUKUDA) confirmed an incident that a large number of phishing emails were sent out to external email addresses using email accounts of UEC because a PC of Institute for Laser Science was cracked. We sincerely apologize to bother all of you if you have a nuisance the incident may have caused.

The PC did not store any personal information, such as student data. Therefore, any information has not leaked.

We deeply regret that the incident has occurred and are keenly aware of how important a sufficient enhancement of security measures for information device against unauthorized access is.

From now on, as the university, we strive to prevent further unauthorized access to the information device connected to the network from the outside.

After we have confirmed this incident, we reported the details to the police immediately. Also, we are currently consulting with them how we will handle this matter.

１．Summary of this incident

A PC of Institute for Laser Science was cracked on May 3, 2016. Mass amounts of phishing emails were sent out to total 2.8 million external email addresses by a spammer using email accounts of UEC which imitated some bank's email address from May 3 until 4 to steal IDs and passwords for online banking of overseas bank.

This incident occurred because the password of the cracked PC was easily guessed by the spammer. In addition, the access restriction did not set up properly on the PC.

We confirmed that the phishing website linked in the phishing email has been closed since May 9.

２．Sender address (× is any single character)

- ko×@cs.uec.ac.jp
- 【Name of bank】@cs.uec.ac.jp
- 【Name of bank】s@cs.uec.ac.jp

３．Contents of the phishing email

The summary of the contents is as follows:

- Changing the bank's confirmation system for online banking service on May 4
- Requiring login from URL in the email to confirm the user information.
- Online banking service temporary unavailable unless the user information is confirmed through the URL

４．Emergency response measures

UEC disconnected the cracked PC to stop the phishing emails on May 4.

５．Further measures

UEC informs and explains this incident to those concerned through UEC homepage and our campus notice board etc. We also consult on any inquiry of this incident by email or telephone as stated below.

６．Measures to prevent recurrent

To ensure to prevent this sort of incident from ever happening again in future, UEC requires all faculty members and students to change their passwords of PCs and network services to safe and secure one. In addition, as our information security measures to further improve the network security, we stop using unnecessary network services, delete unused accounts from our network system and restrict access to our network system to block unauthorized access from external network.

【Contact】

Section in Charge：Information System Section, General Affairs Office, The University of Electro-Communications
Phone：+81-42-443-5034
Opening Hours：9:00～18:00（except Saturday, Sunday and National holidays）
Email：abuse@uec.ac.jp

【Press Contact】

Section in Charge：Public Relations Section, General Affairs Office, The University of Electro-Communications
Phone：+81-42-443-5019
Opening Hours：9:00～18:00（except Saturday, Sunday and National holidays）
Email：kouhou-k@office.uec.ac.jp