

03

## 메일 내 링크 URL 확인

해킹메일 중 링크 클릭을 유도하여 계정정보를 탈취하는 경우가 많아  
**클릭 전 반드시 정상적인 URL**인지 확인하셔야 합니다.

### <KAIST 실제 사례 - 비정상적인 URL>

☆ 최종 경고: kaist.ac.kr입니다



kaist.ac.kr <mailserv3r@sjdept.com> 02.21 13:52 ①

받는 사람: 임영민

#### 중요 보안 업데이트

여보세요? 여기는 kaist.ac.kr 입니다.

계정을 안전하게 보호하기 위한 노력의 일환으로 계정에서 비정상적인  
활동이 감지되었으며 보호를 위해 계정을 보류하고 있습니다.

아래 버튼을 클릭하여 [mailserv3r@kaist.ac.kr](mailto:mailserv3r@kaist.ac.kr) 이메일을 확인하고 계정을 잠  
금 해제하세요.

**마우스 올리면 링크 표기**

이메일 확인 [mailserv3r@kaist.ac.kr](mailto:mailserv3r@kaist.ac.kr)

[https://gandoki.s3.eu-north-1.amazonaws.com/control\\_bdd.html?login=mailserv3r@kaist.ac.kr](https://gandoki.s3.eu-north-1.amazonaws.com/control_bdd.html?login=mailserv3r@kaist.ac.kr)

링크 위 마우스를 올리면 하단에 URL이  
표기됩니다. **수상한 URL일 경우**  
**신고**해주시기 바랍니다.



**KAIST 정보보안팀**