

Account Takeover

Spotting the Threat



The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials. Cybercriminals use brand impersonation, social engineering, and phishing to steal login credentials and access email accounts.

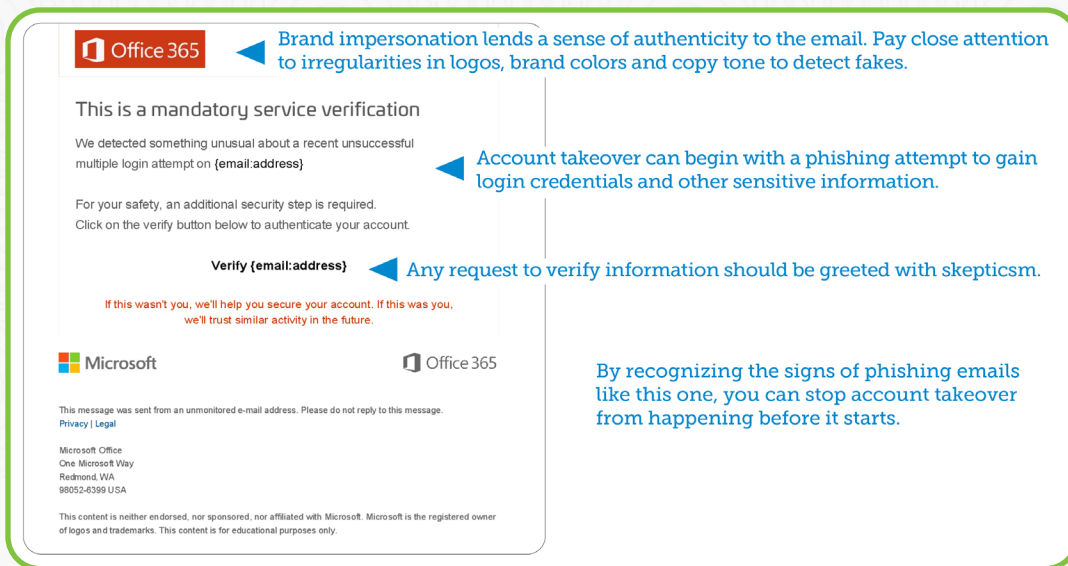
Once the account is compromised, hackers monitor and track activity to learn how the company does business, the email signatures they use, and the way financial transactions are handled. This helps them launch successful attacks, including harvesting additional login credentials for other accounts.

Combatting account takeover requires a variety of strategies:

- Identifying the signs of phishing emails that could lead to account compromise.
- Recognizing signs of brand impersonation and url spoofing.
- Fortifying yourself against social engineering tactics by knowing how social engineers operate.

The sample shown is typical of emails that lead to account takeover.

Example



Office 365 Brand impersonation lends a sense of authenticity to the email. Pay close attention to irregularities in logos, brand colors and copy tone to detect fakes.

This is a mandatory service verification

We detected something unusual about a recent unsuccessful multiple login attempt on (email:address)

Account takeover can begin with a phishing attempt to gain login credentials and other sensitive information.

For your safety, an additional security step is required. Click on the verify button below to authenticate your account.

Verify (email:address) Any request to verify information should be greeted with skepticism.

If this wasn't you, we'll help you secure your account. If this was you, we'll trust similar activity in the future.

Microsoft **Office 365**

This message was sent from an unmonitored e-mail address. Please do not reply to this message.
[Privacy](#) | [Legal](#)

Microsoft Office
One Microsoft Way
Redmond, WA
98052-4399 USA

This content is neither endorsed, nor sponsored, nor affiliated with Microsoft. Microsoft is the registered owner of logos and trademarks. This content is for educational purposes only.

By recognizing the signs of phishing emails like this one, you can stop account takeover from happening before it starts.