24.01.2020

Microsoft data leak

250 million Microsoft support data have been publicly accessible in December, enabling fraudsters to potentially abuse these for phishing mails or telephone scams. Protect yourself!

Over the period from 5th to 31st December 2019, 250 million entries containing Microsoft customer support data have been left unprotected and publicly accessible. Once notified, Microsoft is said to have reacted and closed this data leak within 24 hours. Customer data affected are purportedly going back as far as 2005. They include chat recordings, e-mail addresses and location data.

The fear now is that fraudsters will be able to abuse this information to draw up plausible spamming or phishing mails. With Microsoft, it would also be conceivable that these data are used by telephone scammers. Fake telephone support by purported Microsoft support staff has been a perennial scam for years. So far it is not known whether any unauthorised people were able to access these data.

How to protect yourself:

- Immediately terminate any unsolicited calls by purported Microsoft, other IT support company or financial institution employees. Never rely on a number shown on your telephone display to be actually correct.
- Always call the official Microsoft, other IT support company or financial institution official telephone number in case of any support queries. These can be found on your bills or account statements.
- Never disclose any confidential information, such as passwords, during telephone calls.
- Never use any links you receive by e-mail, SMS or messenger services, or scan in any QR codes to log into a Microsoft, IT support company or your financial institution site.
- Never fill in any forms received by e-mail asking you to enter log-in information.
- Always enter the address for your online service provider or financial institution log-in page manually via the browser address line.
- Check there is an SSL connection (https://, lock symbol) when calling up a log-in page, and verify that the Internet address shown in the address bar of your browser actually indicates that you have reached the correct page.

Additional information can also be found in our articles on phishing (https://www.ebas.ch/phishing) and fraudulent support calls (https://www.ebas.ch/en/fraudulent-support-calls/) .

Learn how to effectively protect yourself against Internet fraudsters by attending our course (https://www.ebas.ch/course) !

Copyright – All rights reserved. Lucerne School of Information Technologies