Fraudulent support calls

Criminals don't just limit themselves to the Internet to obtain confidential information. They increasingly also use the phone. This type of crime is called "vishing".

Protect yourself by:

- immediately terminating any unsolicited calls by purported Microsoft, other IT support company or financial institution employees.
- never relying on a number shown on your telephone display to be actually correct.
- never disclosing any personal data such as passwords or credit card details to any other person.
- always calling the official Microsoft or other IT support company's official telephone number.
- only ever contacting your financial institution via their official telephone number, which can for instance be found on your account statements.

The term "vishing" stands for "voice phishing". Similar to classic phishing and with the help of faked facts, people are tricked into disclosing confidential information or installing alleged security software – while in reality, this is malware.

During such phone calls, attackers often pretend to be a Microsoft, an IT support company or financial institution employee. A caller might for instance claim that a virus infection has been found or that there is another technical problem. These fraudsters intend to convince their victims to either download software from the Internet or visit a faked website, which does however look strikingly authentic.

Both ways, criminals are able to obtain direct access to their victim's device, to then for instance capture passwords or view, copy and process any data stored on their computer unnoticed. Some fraudsters may even ask for a fee payment for their so-called "support service", so that they obtain credit card numbers; of course for subsequent fraudulent use.

Callers often speak broken English. Since telephone numbers can be electronically manipulated, victims' telephones might even display a company's correct telephone number.

It is ever more frequently the case that such purported employees will ask victims to call themselves. To do so, victims are shown advertising windows (pop ups) when surfing the web, informing them that there are problems. The same pop-up will also show a Swiss telephone number victims are to call to resolve the "problem."

If it is too late already, and you have already allowed the access to your device, immediately disconnect it from the Internet, or switch it off. Only switch your device back on once you have deactivated the network (e. g. switched the WLAN off) and then immediately check the whole hard drive with antivirus software. You should also change all passwords. In case you are unsure or need to, please ask a specialist for help.

If you have already disclosed sensitive information (for instance credit card or bank data), please immediately contact your credit card company and/or your financial institution as well as the local police.

Copyright © 2024 – All rights reserved. Lucerne School of Information Technologies

*Microsoft, other IT support companies or financial institutions **never** make any unsolicited phone calls to private users to offer technical support! In such cases, customers must always take the initiative themselves.*

Info sheet:

(https://www.ebas.ch/wp-content/uploads/2019/09/supportSKP_en.pdf)

Copyright © 2024 – All rights reserved. Lucerne School of Information Technologies