Data Privacy Detective Podcast – Episode 61: How Not To Get Phished!

Jan 28, 2021

Categories:

Blogs
Podcast
Publications
Technology Blog

Authors:

Joseph J. Dehner

Data theft set new records in 2020. The major causes are not failures of equipment, software, or services. In an estimated 85% of cybercrime, the cause is us. We make careless mistakes as though we were inviting villains into our homes. We let thieves into our IT systems by accident. We get phished.

You get a message on your computer. It may seem to be from a friend, a trusted source, a reliable company, even your boss. It might seek an urgent response about something. How do you avoid dealing with the emailed message without letting a villain into your computer, and so into your personal or business' IT systems? How do you prevent making a mistake that gives a cybercriminal the chance to freeze and hold your personal or your company's IT system for ransom or to hack personal and proprietary information?

Check emailed messages for seven red flags before acting:

Here are seven top tips to avoid being the reason you or your business is the victim of data theft.

- Bad spelling
- Bad grammar
- Nonsense in the subject line
- Incorrect domain name in images and links (hover over a link without clicking to reveal this)
- Pressure tactics to scare you into acting fast
- Unexpected message
- Unexpected attachments or links in the message

Learning how to spot these common warning signs will make you a better guardian of personal and business data. The information in this episode has been turned into a 5-minute video to help you avoid becoming a phishing victim.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons