Last updated:
November 25, 2021

Source:
The SecDev Foundation

Don’t Let Phishing or Malware Get You

Don’t fall for phishing:

- **Remain skeptical**
  When something is too good to be true, it probably isn’t.

- **Don’t download attachments from sources you don’t trust**

- **Don’t click on links without checking them**
  If you hover your mouse over a link in an email or on a webpage, you will see the full website address. This can help you decide whether or not you want to click that link.

  Before clicking on a link that you find even a tiny bit suspicious, scan it with a link scanner such as Norton Safe Web (https://safeweb.norton.com/) that lets you enter the URL of a suspicious link and check it for safety.

- **Slow down to think**
  Take time to think over all “urgent” requests for information or financial transfers and discuss such requests with other colleagues when possible.

- **Verify identity**
  Always double-check that people requesting information or financial transfers are those who you think they are. Call them or get in touch via a secure messaging platform.

- **Keep your anti-virus and firewall up-to-date and running**

Don’t let malware infect your device:

- **Use antivirus software and keep it up-to-date**

- **Keep your software and hardware up-to-date**

- **Use a non-admin account**
  Malware can be particularly devastating for your device and data on it when you are logged in an administrator account. It is a good idea to create a user account with limited

privileges on your computer and use it for regular daily tasks. When you are signed in to an account with restricted privileges, it is much harder for malware to find a way into your device and make system-wide changes.

- **Know what you install**

- **Don’t download attachments from sources you don’t trust**

- **Check links before clicking**
  If you hover your mouse over a link in an email or on a webpage, you will see the full website address. This can help you decide whether or not you want to click that link.

  Before clicking on a link that you find even a tiny bit suspicious, scan it with a link scanner such as Norton Safe Web (https://safeweb.norton.com/) that lets you enter the URL of a suspicious link and check it for safety.

- **Don’t trust pop-up messages**
  You surf the Internet and suddenly there is a pop-up window telling you that your computer has been infected and recommending that you download some software to protect your device. Do not fall for this.

- **Think twice before inserting removable media into your device**
  Malware often travels across different devices via removable media such as USB memory sticks, external hard drives, flash memory cards and so on. Never insert such a device into your computer if you do not know where it came from. When you have to use a removable media device and know where it came from, it is a good idea to use an antivirus program to scan the device before opening it.