MALWARE: Think Before You Click

Here is an explanation about malware and how you can take steps to protect yourself and your devices from being compromised.

Malicious software – or "malware" for short – is a broad class of software built with malicious intent.

Law enforcement agencies and security experts have seen an increase in a certain kind of malware known as "ransomware," which restricts someone's access to a computer or a smartphone – literally holding the device hostage – until a ransom is paid. While businesses have been targeted more than consumers to date, many home computer users have been victims of ransomware.

The most common way malware spreads is when someone clicks on an email attachment – anything from a document to a photo, video or audio file. Criminals also might try to get you to download malware by including a link in the wording of an email or in a social media post which directs you somewhere else, often to an infected file or Web page on the Internet. The link might be part of a story that sounds very provocative, such as one with a headline that says, "How to Get Rich" or "You Have to See This!" Malware also can spread across a network of linked computers, be downloaded from an infected website, or be passed around on a contaminated portable storage device, such as a thumb drive or flash drive. Here are reminders plus some additional tips on how to generally keep malware off your computer.

- **Don't immediately open email attachments or click on links in unsolicited or suspicious-looking emails.**
  Think before you click! Cybercriminals are good at creating fake emails which look legitimate but can install malware on your device. Either ignore unsolicited requests to open attachments or files or independently verify that the supposed source did send the email to you (by using a published email address or telephone number).
- **Install good anti-virus software which periodically runs to search for and remove malware.**
  Make sure to set the software to update automatically and scan for the latest malware.
- **Be diligent about using spam (junk mail) filters provided by your email provider.**
  These services help block mass emails which might contain malware from reaching your email inbox.
- **Don't visit untrusted websites and don't believe everything you read.**
  Criminals might create fake websites and pop-ups with enticing messages intended to draw you in and download malware.
- **Be careful if anyone – even a well-intentioned friend or family member – gives you a disk or thumb drive to insert in your computer.**
  It could have hidden malware on it. Scan all storage devices prior to opening any files to your device.

Heritage BANK

Information provided by the FDIC