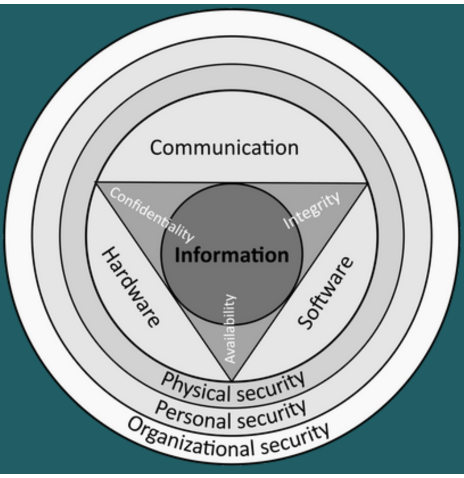
RICE

Cybersecurity: How to Identify Threats and Ways to Protect Against Them

Tips and Facts on Detection and Protection



WHAT IS CYBERSECURITY

Cybersecurity, a facet of Information Security, is a term used that encompasses many categories. It is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this (Oxford Dictionary, 2022). This field has grown in significance due to the creation and expansion of computers, networks, the internet, and smart devices like phones, tablets, watches, virtual reality, and artificial intelligence in present-day household items (Google AI, Apple AI, and Amazon AI).

MALWARE AND RANSOMWARE

Malware and Ransomware infect servers and encrypt files. Malware is any type of code or software made with malicious attempt. Ransomware holds system data hostage and demands a form of payment from the user.

678 million	Number of detected malware attacks in year 2020
236 million	Number of detected ransomware attacks in year 2022
85%	Percentage of emails that are detected as spam at a daily rate
323,972	Number of people who were victims of phishing in 2021
15 million	Number of United States residents that have their identities stolen

SPAM AND PHISHING

Spam can take many forms, but it is defined as "unwanted, unsolicited, or undesirable messages and emails." Phishing is an "attempt to get sensitive information" (Know the Types of Cyber Threats, 2022). Most forms of spam and phishing come in emails, be that sent to personal, work, or school emails. Phishing and spam go hand in hand because oftentimes a spam email will be a phishing attempt.

IDENTITY THEFT

Identity Theft, according to the United States government, happens when criminals steal personal information from a different person to commit fraud; the information can then be used to apply for credit, file taxes, or get medical services (2022). It encompasses many forms of cyberattacks.

DETECTION

Each category previously mentioned can be detected if the early warning signs are caught within a notice period. It's important to regularly check for the issues listed below.

Malware and Ransomware

Keep your eyes peeled for

- Websites with domains that end in '.to' or '.dad'. They typically have malicious code written within.
- Websites with multiple spelling errors on their page.
- Suspicious error messages that pop up on a personal device or email that demand any monetary value.

Spam and Phishing

Keep your eyes peeled for

- Websites with an overuse of ad spacing.
- Suspicious emails that contain ads from websites you recently visited. You may have enabled cookies on your personal device and are being tracked.
- Emails that ask you to download random programs. These are called Trojan Horses and they are designed to damage your data or network.

Identity Theft

Continuously check your

- Credit reports once a year. They can be ordered for free from this website: Annualcreditreport.com.
- Billing cycles.
- Social Security number and make sure to keep it private.

REFERENCES AND SOURCES

- Computer security picture - Wikipedia
- What's On the Other Side of Your Inbox - 20 SPAM Statistics for 2022 (dataprot.net)
- The Latest 2022 Phishing Statistics (updated November 2022) | AAG IT Support (aag-it.com)
- Identity Theft Statistics: 15 million victims a year | www.IdentityTheft.info
- Number of ransomware attacks per year 2022 | Statista

PROTECTION

The following protection techniques can be used as countermeasures in the event that an issue comes up.

- Regularly back up data and verify the integrity of those backups.
- Ensure antivirus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Only download software—especially free software—from trusted sites.
- Protect accounts by using multi-factor authentication.
- Update sharing and firewall settings when using public wi-fi networks. Use a virtual private network (VPN) when on public Wi-Fi.
- Shred receipts, credit offers, account statements, and expired credit cards. This can prevent "dumpster divers" from getting personal information.
- Freeze credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange for free.
    - The Experion App is a great tool for this.

Report Malware and Ransomware attempts to the Internet Crime Complaint Center at www.IC3.gov.

Report Spam and Phishing attempts to the Federal Trade Commission website at ReportFraud.ftc.gov and the Anti-Phishing Working Group at reportphishing@apwg.org.

Report Identity Theft attempts to the Federal Trade Commission at IdentityTheft.gov and by phone at 877-438-4338.

CONTACT

✉ kar15@rice.edu

📍 Computational Applied
Mathematics and Operations
Research Department