Phishing detection and password managers

Prishtina Open Source Festival
7-8 December 2019
Slide design inspired by Timo

About me

- UI/UX Developer at Ura Design
- Member at Open Labs Hackerspace, Open Source Design and The Document Foundation
- Ambassador at the Fedora Project
- Privacy & Security “Consultant”

Addicted to hacking on things

Agenda

- What is phishing and the most used methods
- How phishing works
- How to detect phishing without having to be a tech geek
- Tips & Tricks
- Online account management and proper OPSEC (Operations Security)
- Password managers, 2FA & compartmentalization
- Questions?

Phishing

“Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication”

Phishing types

- Spear phishing
- Whaling
- Clone phishing

- Link manipulation
- Filter evasion
- Website forgery
- Covert redirect
- Social engineering
- Voice phishing

How to detect phishing

- Check links on emails you receive and also the email headers
- Use an adblocker/content blocker with extra lists that block well-known phishing and malware sites (uBlock Origin on medium mode recommended)
- Do not enter your personal information immediately upon being asked
- Triple check the URL of the site and the SSL certificate etc.

Anti-phishing techniques

- User training
- Technical approaches
  - Filtering out phishing mail
  - Browsers alerting users to fraudulent websites
  - Augmenting password logins
  - Monitoring and takedown
  - Transaction verification and signing
  - **Multi-factor authentication**
  - Email content redaction
- Legal responses

OPSEC

“Operations Security is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.”

The OPSEC process

- Identification of Critical information
- Analysis of Threats
- Analysis of Vulnerabilities
- Assessment of Risk
- Application of Appropriate OPSEC Measures

Password Managers

- Open source solutions which are audited
- Offline-only database should be preferred
- Online synchronization only with trusted systems
- Strong master password necessary and unique
- Extra authentication means are nice to have (Yubikey, keyfile etc)

Preferred software

- KeePass (official software)
- KeePassXC (multi arch and cross platform)
- KeePassDX (Android version)
- KeePassium (iOS version)
- Bitwarden (audited, selfhosted option available, extensions available)

2 Factor Authentication

- USE IT USE IT USE IT USE IT USE IT USE IT
- DO NOT SHARE IT WITH ANYONE
- Subset of multi-factor authentication, a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are.

Preferred Software

- Once again, offline-only software is preferred
- KeePass (any of them, plugins available for TOTP)
- AndOTP (Android app)
- FreeOTP (iOS app)

All the above mentioned apps have export/import capabilities

Compartmentalization

“Compartmentalization is a subconscious psychological defense mechanism used to avoid cognitive dissonance, or the mental discomfort and anxiety caused by a person's having conflicting values, cognitions, emotions, beliefs, etc. within themselves. ”

In the digital world

- Separate identities and don’t mix (work with school, work with friends/family etc)
- Do not reuse the same username/email for everything
- Could go further as in using separate devices

Questions?

Thanks for listening!