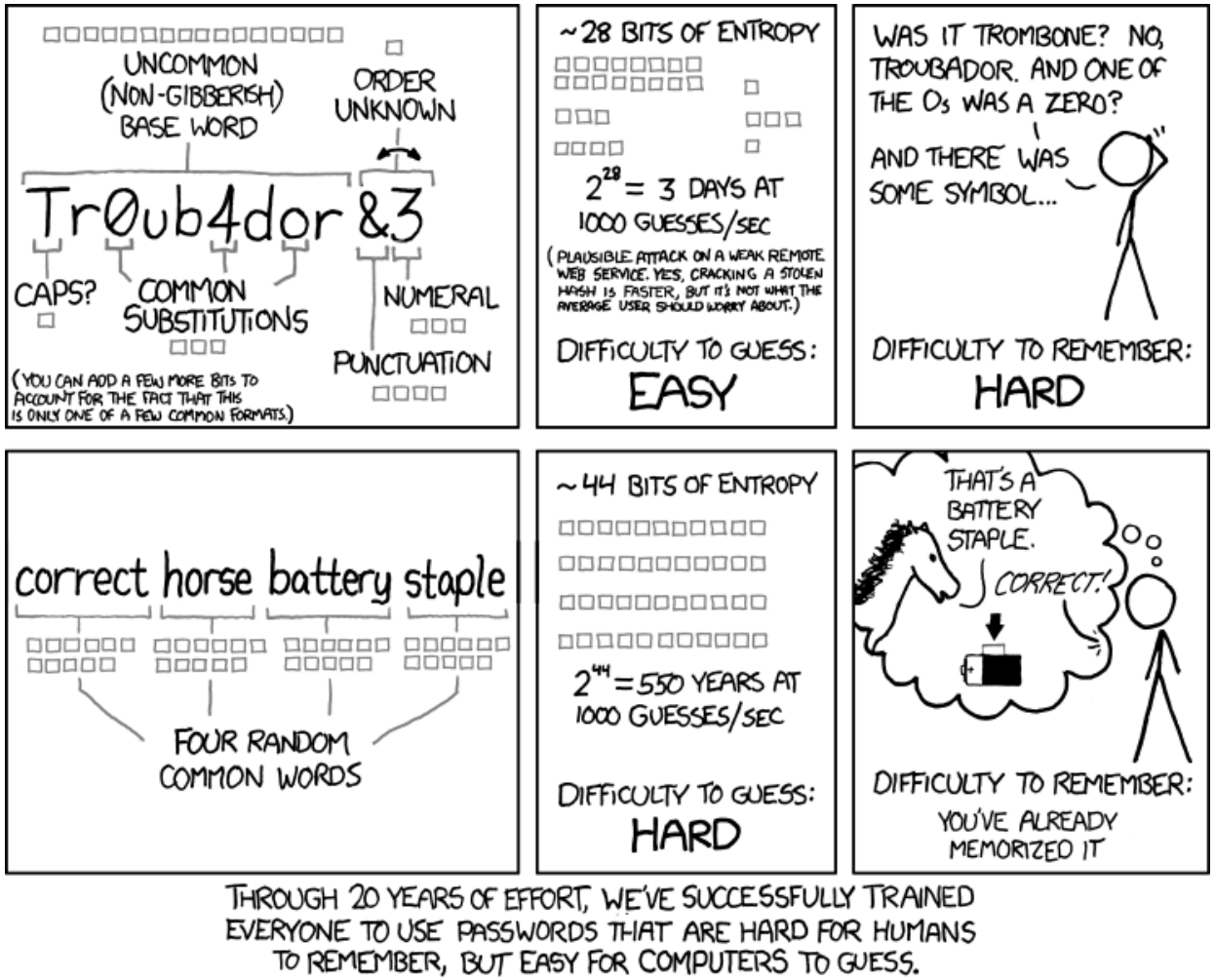
Protecting Your Data and Privacy

- You should encrypt wireless communication by enabling **WPA2 encryption** on your wireless router. Optionally, configure it to **not broadcast the SSID**, which adds an additional barrier to discovering the network.
- In **2017**, a **Key Reinstallation Attacks** (KRACK) in **WPA2 protocol** was discovered, which allows an intruder to break the encryption between the wireless router and the device, access and manipulate the network traffic. It affects all modern, protected Wi-Fi networks.
- To mitigate **update all affected products**: wireless routers and any wireless capable devices with security updates. For laptops or other devices with wired NIC, a **wired connection** could mitigate this vulnerability. A **trusted VPN service** can also be used to prevent unauthorized access to your data while you are using the wireless network.
- See protecting yourself when using wireless networks.
- When using a **public Wi-Fi hot spot** verify whether your computer is configured with **file and media sharing** and that it **requires user authentication with encryption**. To prevent someone from intercepting your information (eavesdropping) use an **encrypted VPN tunnel**.
- **Bluetooth** can be exploited by hackers to eavesdrop on some devices, establish remote access, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth **turned off when you are not using it**.
- **IoT devices** pose an **even greater risk** as most of them still have their **original firmware**. They are very likely to be comprised and when they are, allow access to the local network and data. The best way to protect yourself is to have IoT devices **using an isolated network**, sharing it only with other IoT devices.
- Visit Shodan, a web-based IoT device scanner.

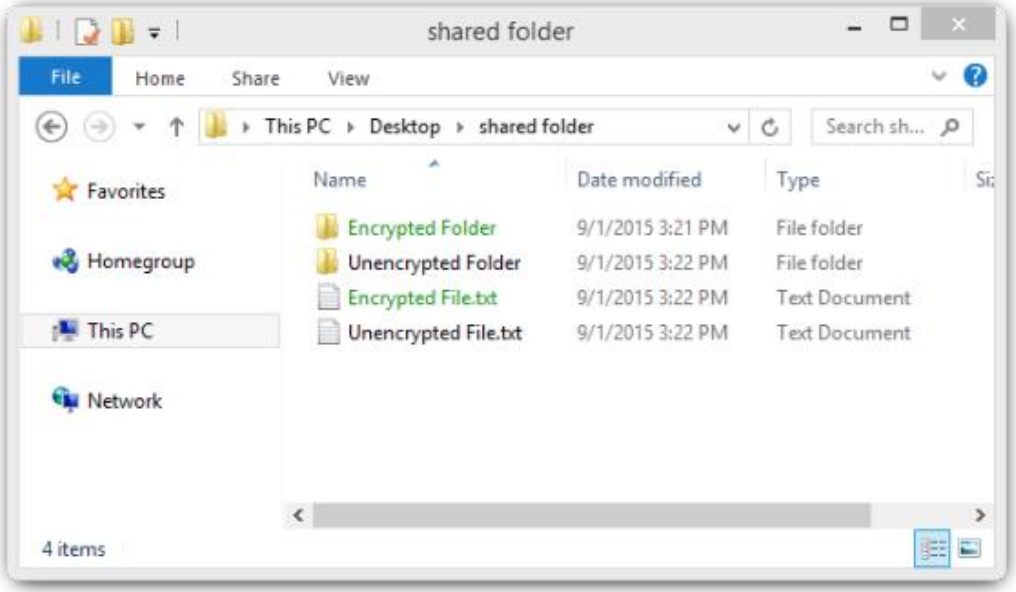
Passphrase Rather Than a Password

- It is **easier to create a long passphrase** than a password. The longer length makes passphrases **less vulnerable** to dictionary or brute force attacks. Furthermore, a passphrase maybe **easier to remember**, especially if you are required to change your password frequently.
- United States National Institute for Standards and Technology (**NIST**) published **improved password requirements**. NIST standards are intended for **government application** but can also serve as a standard for others as well. The new guidelines aim to provide better user experience and put the burden of user verification on the providers.
- [Learn more about the NIST password requirement.]



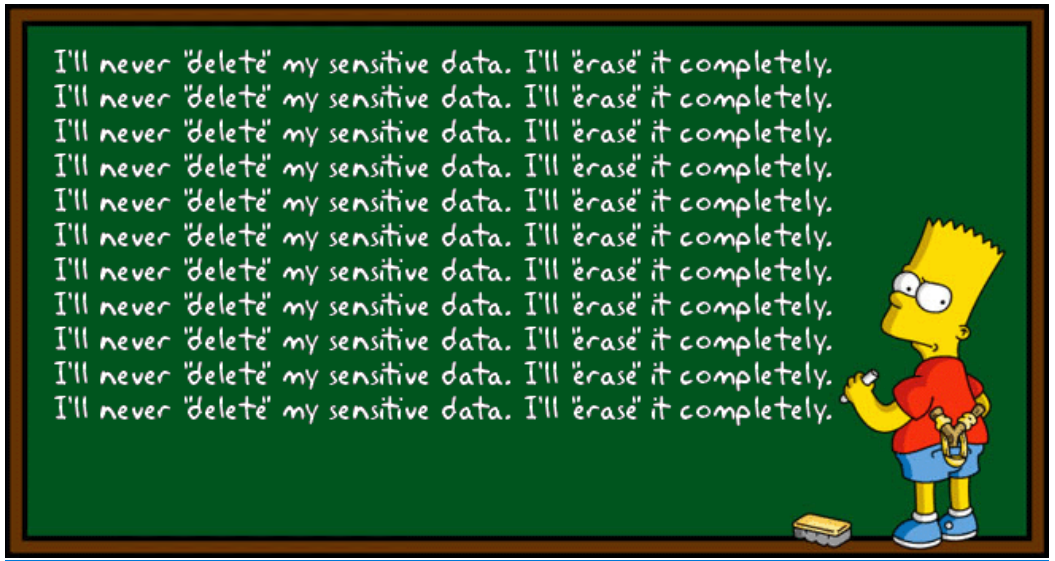
Encrypt and Backup Your Data

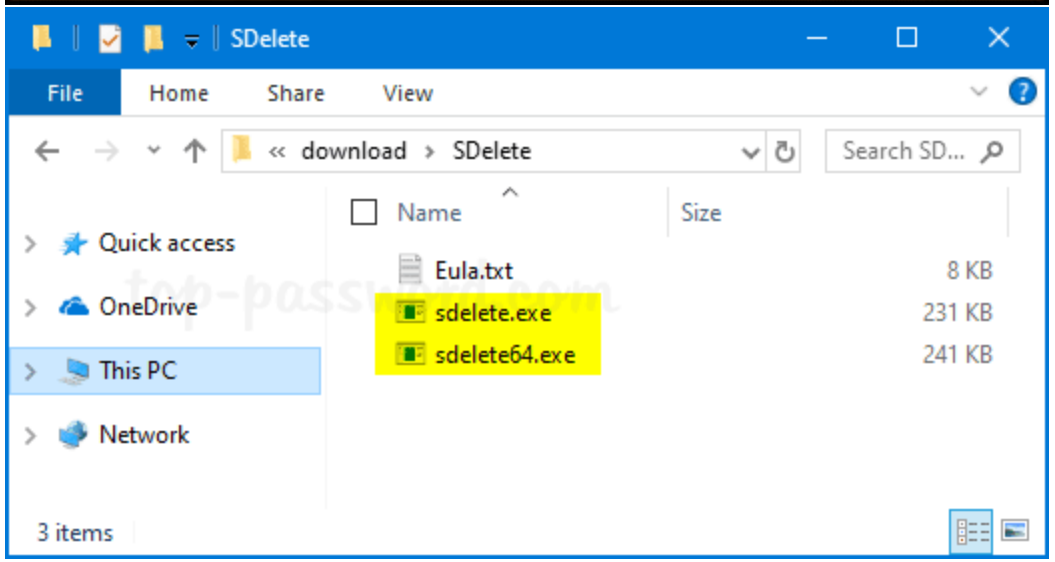
- If a malicious application infects your computer, it could steal valuable information, such as account numbers, passwords, and other official documents. Criminals may decide to simply encrypt your data and make it unusable until you pay the ransom.
- **Encryption** is the process of converting the information into a form such that only an authorized person with the password can decrypt the data and access it in its original form. **Software programs** are used to encrypt files, folders, and even entire drives. **Encrypting File System (EFS)** is a Windows feature that can encrypt data.
- Having a **backup** may prevent the loss of irreplaceable data. You can decide to copy all of your data to a **network attached storage device (NAS)**, a simple **external hard drive**, or maybe select only a few important folders for backup on **thumb drives**, or **CDs/DVDs**.
- With a **cloud storage service** like Amazon Web Services (AWS), you have access to your backup data as long as you have access to your account.



Deleting Your Data Permanently

- When you move a file to the recycle bin or trash and **delete** it permanently, the file is only **inaccessible from the operating system**. Anyone with the right **forensic tools can still recover the file** due to a magnetic trace left on the hard drive.
- In order to **erase** data so that it is no longer recoverable, the **data must be overwritten with ones and zeroes multiple times**. The program **SDelete** from Microsoft, **Shred** for Linux, and **Secure Empty Trash** for Mac OSX claim to have the ability to remove sensitive files completely.
- The only way to be certain that data or files are not recoverable is to **physically destroy the hard drive** or storage device. It has been the folly of many criminals in thinking their files were impenetrable or irrecoverable.





Authentication

- Online services use **two factor authentication** to add an extra layer of security for logins. Besides the username and password, it **requires a second token**, such as a:
- **Physical object** - credit card, ATM card, phone, or fob.
- **Biometric scan** - fingerprint, facial, or voice recognition.

- Open Authorization (**OAuth**) is an open standard protocol that allows an end user's credentials **to access third party applications without exposing the user's password**. OAuth acts as the middle man to decide whether to allow end users access to third party applications.
- Using **secret tokens** prevents a malicious application from getting your information and your data.