Twitter Thread by The BooneNator

The BooneNator
@DBooneNator

Information Security Framework, Pt I: the Basics:

Let's start with the simple things.

1. Keeping up-to-date on all things software-related on the machine should be paramount.

Not just operating system updates though.

Software updates for things like word processing programs, music players, email clients, etc.

Kernel and BIOS updates for the machine itself.

If you want to check for the newest BIOS update, look at your computer hardware, visit the vendor's site, and they will have BIOS downloads available, as well as the date they became available.

Keep in mind, some updates on the BIOS itself aren't always necessary.

If the vendor recommends "Not updating if stability isn't a problem, then don't do it"

2. Next, let's talk about things that may communicate over the local network or within a short proximity, such as Bluetooth, airdrop, etc.

If you're not using them, turn them off.

Airdrop is especially troublesome because often I'll be at an airport and see dozens of individuals who have airdrop enabled. I recommend setting it to 'Contacts only' unless you're intending to pass a file to someone close to you.

3. Next, let's talk passwords. This one is extremely troublesome for a good portion of the population anywhere. Often we see people that include names of people they're close to, with a couple numbers of interest.

The number could be their birth year, the year they graduated high school/college, or an event of significance in their life.

Regardless of what it is, these passwords should be complex enough for an automated brute force-like password attack or dictionary attack.

Dictionary attacks leverage a text file of common dictionary words to run the attack. It is typically quicker if the password isn't expected to contain combinations of numbers and special characters. It can be quicker only for the lowest hanging fruit.

Brute force simply runs a number of permutations per second until it finds the password of interest. While it's slower, it eventually breaks a password if it's too short or simplistic.

Due to the concept of Moore's law, we have technology now that can run brute force attacks much quicker, although to be honest there are easier ways to retrieve passwords. More on that later.

The next issue people tend to have is using the same password for most accounts.

BIG mistake. Here's why:

IF an APT (Advanced Persistent threat) is ran on a large company, such as things we've seen in the last five years, they may be able to retrieve the email AND password of that account.

Since many people use identical passwords across the board, this can cause a domino effect across the board.

If they know your email and a common password you use, they can start trying it across the board, going to common sites where folks do business at.

Whether that be Amazon, Gmail, Ebay, etc, it doesn't matter.

By taking advantage of this opening, they could gather even more info on you, whether that be addresses, birth dates, or even connections to other accounts with significant PII (Personally Identifiable Information).

So how do you manage remembering different passwords for different accounts?

Simple. Use a password manager.

Here's how it works: You create a database of passwords, label what site they're for, URLs for the site of interest, email it's linked to, and other additional details in a notes section (For additional details we'll cover later).

You can also specify expiration times for the password. While simple accounts that don't contain much sensitive information won't need their passwords changed often, it'd be prudent to change passwords of finance-related services at least a few times a year.

Same goes with cloud storage, email, etc.

There are two good options: Keepass and Bitwarden.

Bitwarden is cloud-based, Keepass is not. I personally prefer Keepass as the cloud is a risky place for anything, regardless of how 'secure' they claim they are.

To each their own. Keepass is only available on Windows, but KeepassXC is well maintained for other platforms.

So here's the recommendation: Generate a 20-character password, including special characters and numbers.

Some sites don't like certain special characters allowed in the password, so take note of which ones they allow when creating a password.

Update accounts with sensitive info every six months MINIMUM.