your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

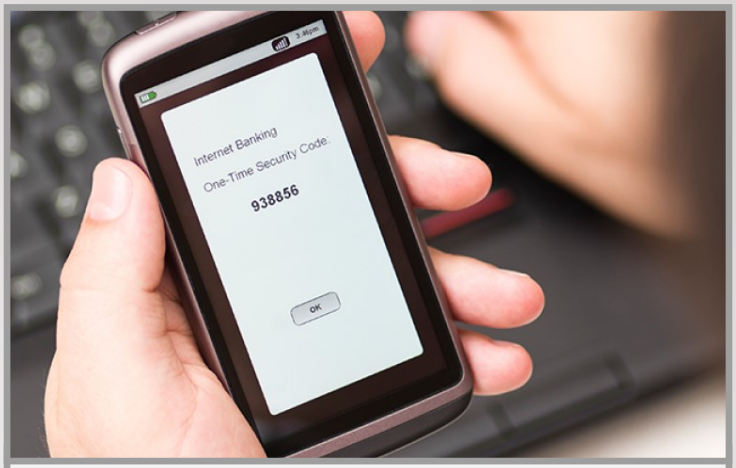
Two Factor Authentication: Your Best Defense

Passwords are frequently hacked, whether it is through brute forcing or phishing attacks, passwords can be scooped up by scammers fairly easily. What you really need is a second way to verify yourself. That's why many internet services offer two-factor authentication. Meaning when you log into a service on the internet, not only will it ask for your password, but it will also verify you are who you say you are through the use of your mobile device's phone number.

Typically a PIN number or one time use code will be sent to your phone, which can be used only once, and is a great added layer of security you can use against fraudulent actors attempting to compromise websites or devices that you regularly sign on to.

If you use Google or Facebook you have no doubt already encountered two-factor authentication (2FA). Implementing two-factor authentication typically takes slightly longer to log in each time on a new device, but worth it in the long run to avoid identity theft, or stolen credentials. Being more secure sometimes means sacrificing ease of access and comfort, but malicious actors count on you being lax in protecting yourself, so never take that chance.

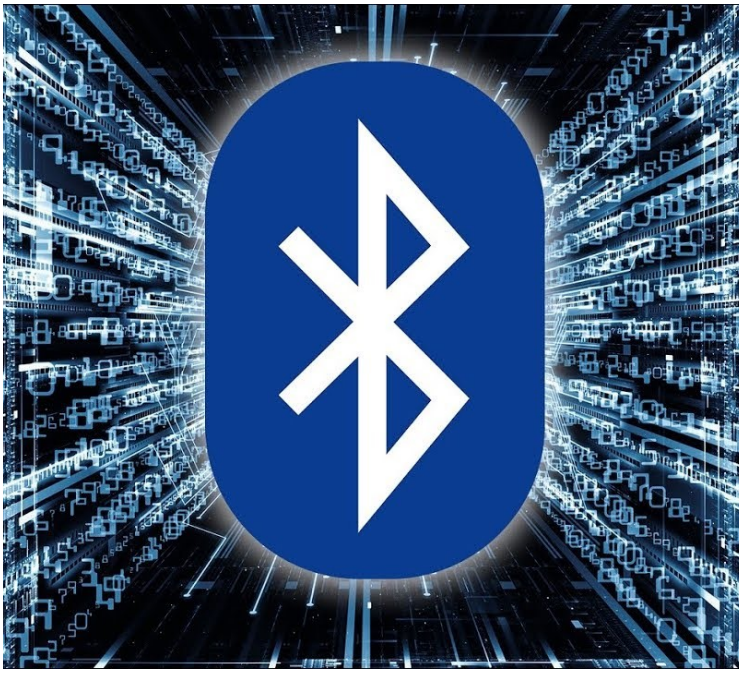
Don't think it'll happen to you? So-called 'credential stuffing' or brute-force attacks can make it easy for hackers to break in and hijack people's



online accounts in bulk. That happens all the time. Dunkin' Donuts, Warby Parker, GitHub, AdGuard, the State Department — and even Apple iCloud accounts have all fallen victim to credential-stuffing attacks in recent years. Adding 2FA to your accounts is another layer of security to help prevent these type of automated log-in attacks. Two-factor authentication also provides another layer of defense against malicious phishing emails. If someone sends you a phishing email that sends you to a false website trying to trick you into logging in with your Google or Facebook username and password, 2FA can still protect you. Only the legitimate site will send you a working two-factor code which means you'll know you're on a fake site when you don't go through the 2FA login steps each time. Consider turning on 2FA for all the sites that you access that supports it.

https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/

Why You Should Turn Off Your Bluetooth When It's Not In Use?



Many people who frequently use Bluetooth speakers, headphones, or other Bluetooth friendly devices typically leave their bluetooth signal turned on out of ease of convenience. Statistics say 40%-50% of people leave their Bluetooth on which leaves them open and vulnerable to many attacks.

A security company called Armis has found a collection of eight exploits, collectively called 'BlueBorne', that can allow an attacker to access to your phone without touching it in less than 10 seconds. Hackers can then run malicious code while staying practically invisible, and will have full control over the device without any user interaction.

The first way to keep yourself safe is to only enable Bluetooth if strictly necessary. Keep in mind that most Bluetooth-enabled headphones also support wired analog audio.

Second, keep your device non-discoverable. Most are only discoverable if you enter the Bluetooth scanning menu. Nevertheless, some older phones might be discoverable permanently.

The attacker has to know your device's Bluetooth MAC address, or network-interface identifier. Bluetooth devices generally broadcast the MAC address only when they want to be found by other devices, and you can turn that off.

Go into your device's settings, find the wireless or Bluetooth settings, and disable "Discoverable" if you can. You'll still be able to link to Bluetooth devices you've already paired with, but not to new Bluetooth devices.

Rest easy, this flaw has not been exploited in the wild, and its discoverers are keeping the details under wraps for the time being so that malicious actors won't be able to start exploiting it right away.

Just know that malicious actors are already reverse-engineering this month's patch to try to find what got fixed and how to exploit it. Stay one step ahead of them!

https://techcrunch.com/2017/09/12/new-bluetooth-vulnerability-can-hack-a-phone-in-ten-seconds/

PROTECT YOUR INFORMATION

UNIQUE DEVICE, UNIQUE PASSWORD

KEEP SEPARATE PASSWORDS FOR EACH DEVICE YOU USE. KEEP A LIST OF PASSWORDS IN A SAFE, SECURE LOCATION.

Most people have a cell phone and other devices to manage work and their personal business. If you use a cellphone, a work computer, a tablet, and a home computer, ALWAYS make sure these devices have unique logon passwords. Besides making the passwords unique, make sure to they are at least 8 characters long, but consider 12-17 characters where feasible to improve your security posture. Best practices for password composition should include two upper case letters, two numbers, and two symbols where your devices allow. Keep your passwords secure, or consider using a password manager to help manage all the passwords you use regularly. Don't be an easy target for malicious actors!