May 2019

SecurityAwarenessNews

the security awareness newsletter for security aware people

Device Maintenance 101

All About Access

The CIA of Device Hygiene

Device Maintenance 101

Device Hygiene Explained

As with automobiles, buildings, and our own bodies, devices require a bit of maintenance. Failing to take basic proactive steps, such as updating apps and deleting and organizing files, can lead not only to degraded performance, but also adds security risks. Here at work, it's your responsibility to follow our organization's policies which are aimed at proper device maintenance. If you're unsure of those policies, please ask! And don't neglect your personal devices. A small commitment to device hygiene yields reliable functionality and reduced security risks.

APPS TO CONSIDER

Keeping your machines clean and running properly doesn't require a ton of work. Here are a few great tools that can help you live a healthy cyber life. As always, never install third-party apps on work-issued devices unless policy allows.

PASSWORD MANAGER

Having trouble remembering all of the logins for all of your accounts? Get a password manager! It creates, stores, and syncs your usernames and passwords across multiple devices.

VPN

Short for virtual private network, a VPN encrypts your internet traffic to prevent cybercriminals from intercepting and stealing your data on public WiFi networks.

ANTIVIRUS

One of the most inexpensive and basic options, software that prevents viruses or malware should be utilized on desktops and devices alike.

FIND MY PHONE

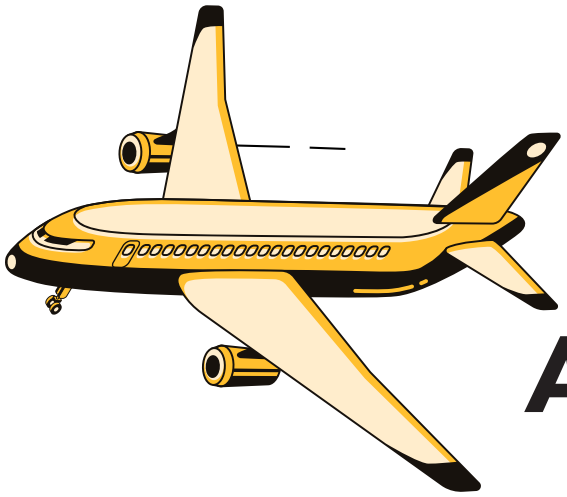
Most smartphones offer a service that allows you to locate your phone from a different device and ping it to ring or completely reset it to default, which erases all sensitive data.

AUTHENTICATOR

Two-factor authentication, or 2FA, requires something you know (your password) plus something you have (your phone) in order to log into an account. Authenticator apps improve on traditional, less secure 2FA methods such as sending codes to your phone number or email address.

Smartphone Security Checklist

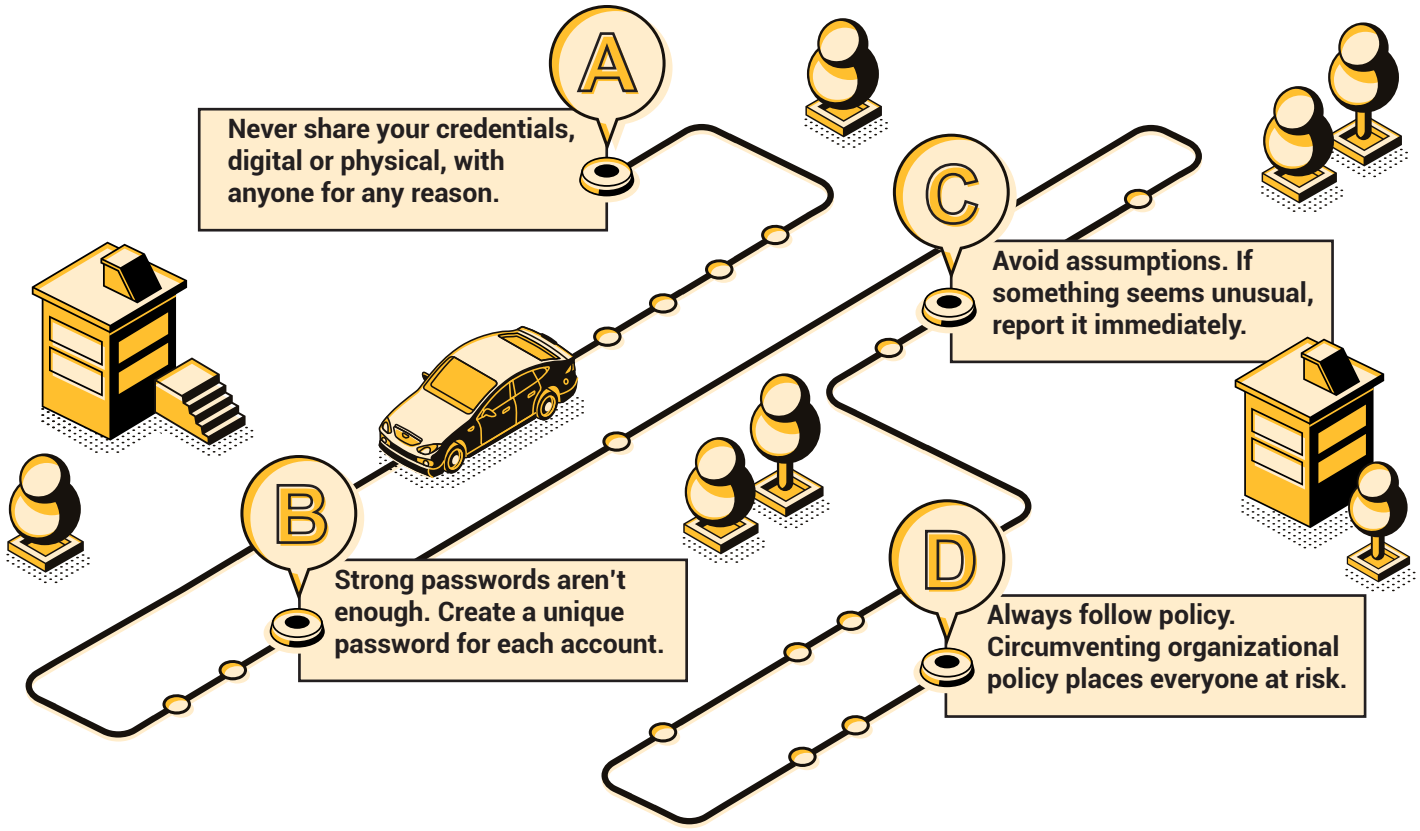
- ☐ **Remove unused apps** *(digital cleaning)*
- ☐ **App permissions reviewed** *(not everything needs access to your location)*
- ☐ **Antivirus software installed** *(it is a computer, after all)*
- ☐ **Password protected and lock screen after a short period of no use** *(it is simple common sense)*
- ☐ **VPN installed** *(never connect to public WiFi without one)*
- ☐ **Auto update enabled** *(updates often patch security flaws and glitches)*
- ☐ **Backed up** *(either to the cloud, a computer, or both)*



ALL ABOUT ACCESS

Imagine taking a flight on an airline that allows any passenger to visit the cockpit at any time. Sounds like a terrible idea, right? Although slightly less threatening, that same concept flies in information security. Every member of our organization has been granted some level of access, but not every member has access to the payroll database, for example. Proper device maintenance includes respecting and securing access to that device!

Respecting Privileged Access In 4 Easy Steps



What is credential stuffing?

Remember how *every security expert ever* warned against reusing the same password for multiple accounts? Credential stuffing is why. When a data breach spills hundreds of thousands of account credentials (usernames and passwords), cybercriminals use that data to "stuff" websites with automated login requests. Any reused credentials will give criminals additional access to other accounts. Don't let this happen to you! ***Create unique passwords for every single account, and enable two-factor authentication wherever possible.***

Bad USB

Compromising an organization doesn't always require phishing emails or sophisticated technology; sometimes, all you need is a simple USB device and a curious human who plugs it in. Flash drives, keyboards, even USB cables, are all capable of delivering malicious payloads on behalf of social engineers. ***Protect your systems by never plugging in unknown USB devices.*** Make sure you know our policy about plugging in USB devices, and if you *ever* find a random USB device, report it ASAP!

SAC the security awareness COMPANY

THE CIA OF DEVICE HYGIENE

Confidentiality: keeping secrets secret

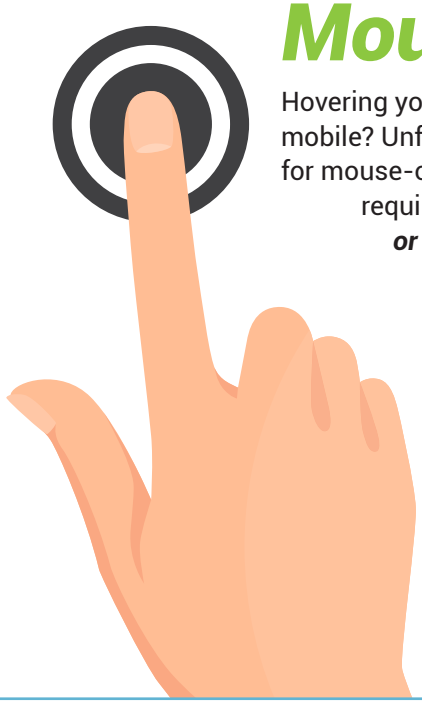
Secrets require strong passwords! Every device should be protected with a strong passcode, and lock screens should automatically initiate after a short period of non-use. That way, if it ends up in a stranger's hands, they won't easily gain access to all of your sensitive info.

Integrity: preventing flaws

One of the easiest security incidents you can avoid is the exploitation of outdated software and firmware. Most devices and apps allow you to enable auto-update, which keeps them functional and upgraded with the latest security patches. Cybercriminals can sometimes use outdated software as a backdoor to gain unauthorized access to devices and computers.

Availability: ensuring secure access

Data is useless if it can't be accessed or located. Since devices can't last forever, we should always view them as temporary and keep them backed up. And don't underestimate the benefits of proper file management! If you can't find it, you can't secure it.



Mouse over on mobile

Hovering your pointer over a link to display the full URL helps keep systems safe. But how is it done on mobile? Unfortunately, with so many different manufacturers and app developers, no standard exists for mouse-overs on mobile. A long-press displays the URL on some devices and some apps. Others require a third-party app to achieve that same function. ***But regardless of whether your device or the app allows you to long-press a URL, it's best to avoid doing so unless you're 100% confident the URL is safe!*** A long-press could lead to an accidental click, which in turn, could lead to a security incident.

POLICY = SECURITY

Every airline enforces a policy that requires cockpits to remain locked during flight. Most businesses are required to provide evacuation routes in the event of an emergency. And our organization develops policies designed to keep data secure and systems safe. ***It's your responsibility to know and always follow our policies. If you need more info, please don't hesitate to ask!***