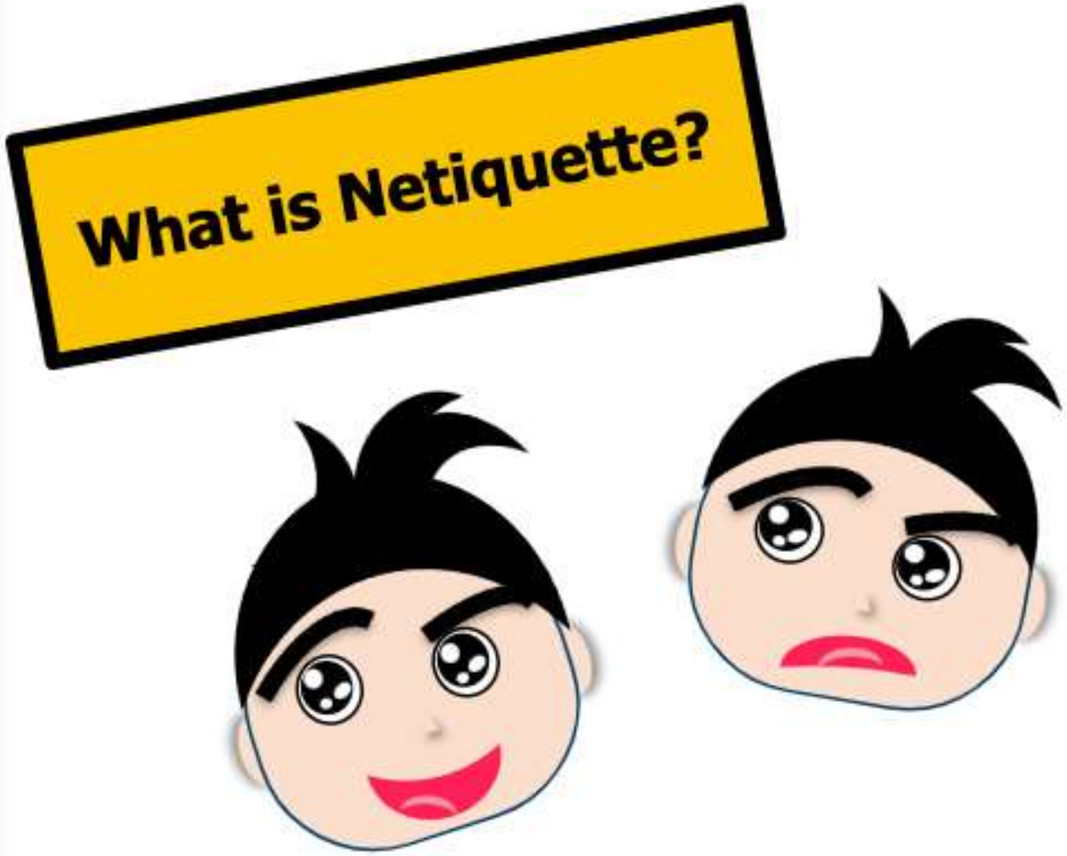
Incident Countermeasure

- ❑ Netiquette
- ❑ Firewall and Software
- ❑ Authentication Mechanisms

NETIQUETTE



https://pumpic.com

NETIQUETTE

A set of rules for acceptable online behavior to help people to communicate more effectively while online, as well as to avoid unnecessary misunderstandings and potential conflicts

NETIQUETTE

What does a good Web etiquette look like?

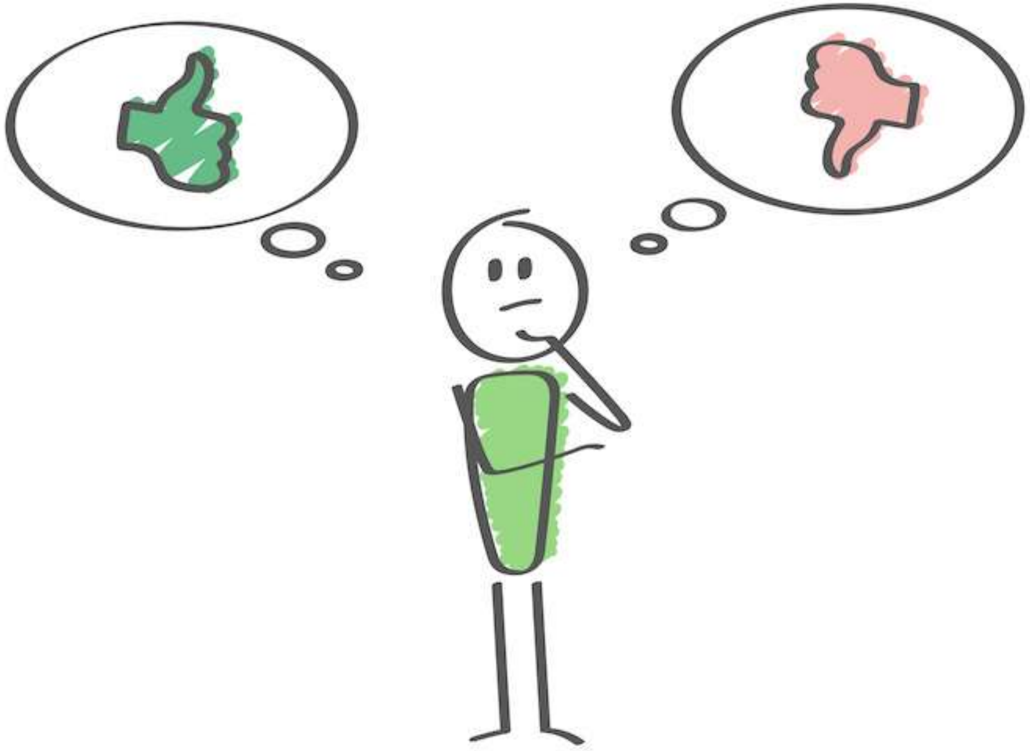
Society

https://www.artspace.com

SOCIETY

Recognizing that the internet is an extension of society

The Internet isn’t a new world in which anything goes, but rather, a new dimension of the world around us.



Applying the same standards online as we do in public

In simple terms, this means that the values society has in place against hate speech, copyright violations, and other forms of theft remain intact. Values around courtesy, kindness, openness, and treating others with the same respect we wish to receive should also be adhered to.

Refusing to empower abuse and harassment while online

Accepting that the laws which are currently in place to protect the rights and dignity of citizens apply online and that where needed, laws are updated to reflect these rights in the extended environment.

Acknowledge cultural differences

Even when national boundaries no longer apply, cultural respect and tolerance should remain. This requires finding a way to accept that the social values and norms of some netizens will not be the social values and norms of all netizens.

NETIQUETTE

Netiquette Golden

https://www.altium.com

Respect people's privacy

Be mindful of your language

Don't be sarcastic

Choose your emojis carefully

Respect other's views

Respect people's privacy

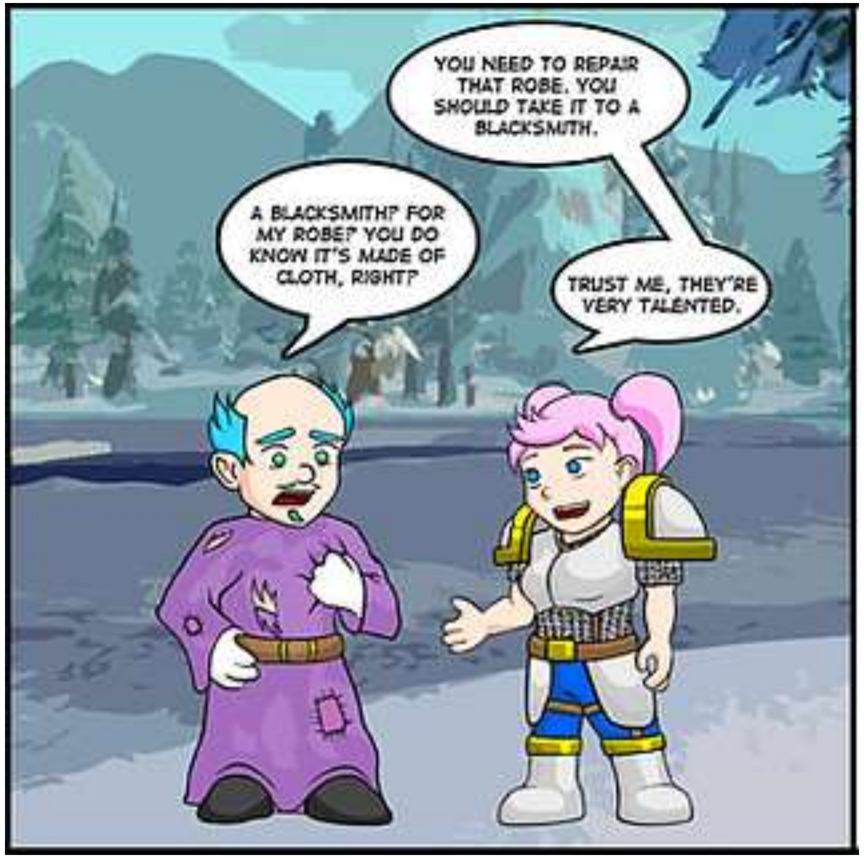
If someone isn't comfortable sharing information with you, try not to push or pressure them into doing so. Never share other people's personal information, such as addresses, phone numbers, or e-mails, without permission as this can be considered doxing.

Note : Doxing refers to the practice of gathering and publishing personal or private information about someone on the internet.

Be mindful of your language

Be aware of the language you use online. Although you might believe it to be funny or harmless, another person might take offense to it or find it upsetting.

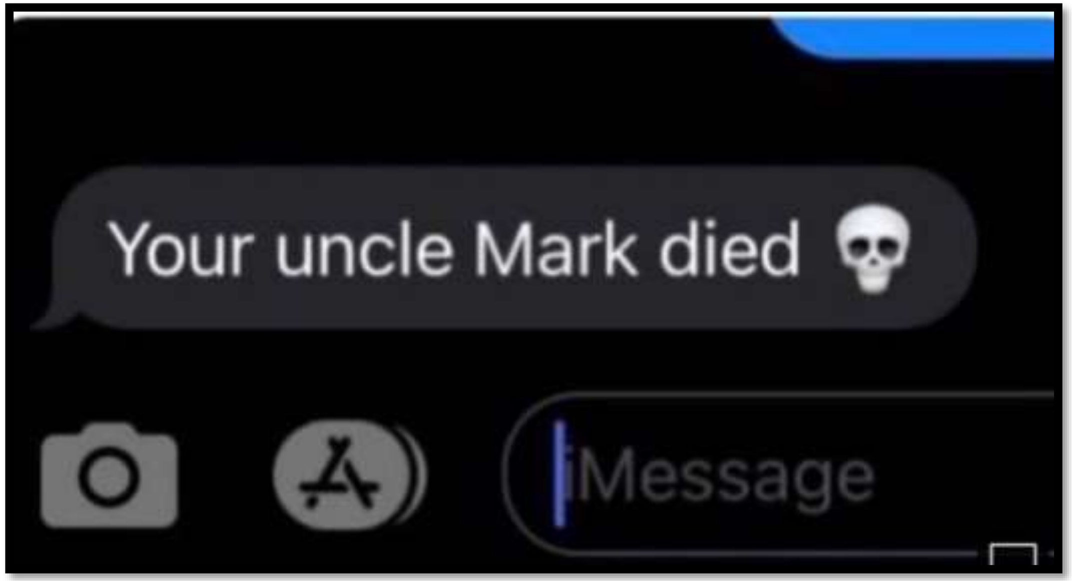
GOLDEN RULES


YOU NEED TO REPAIR THAT ROBE. YOU SHOULD TAKE IT TO A BLACKSMITH.
A BLACKSMITH? FOR MY ROBE? YOU DO KNOW IT'S MADE OF CLOTH, RIGHT?
TRUST ME, THEY'RE VERY TALENTED.

Don’t be sarcastic

Sarcasm doesn’t translate well on the Internet.

Choose your emoji carefully



Your uncle Mark died 💀

Emojis or emoticons have now become a recognized language in their own right. Make sure that if you use emoticons, you are using one that is appropriate for the emotion you are trying to convey as they can easily change the context of an entire conversation.

Respect other's view

The beauty of the Internet relies on varying and diverse opinions and beliefs. Allow others to share their views without the conversation becoming heated or turning into an argument.

Firewall and Software

What is a Firewall?

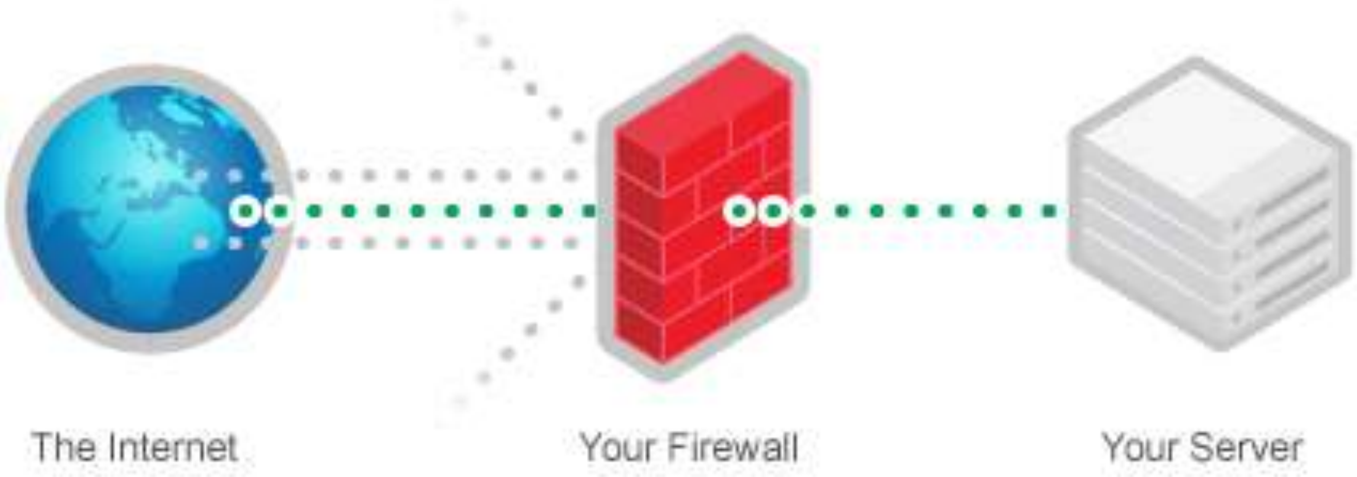
Benefits of Firewall

FIREWALL

A software program which purpose is to defend one’s home or business against electronic threats by screening viruses, hackers and works that infiltrates the computer through the Internet.

FIREWALL

It also serves as a gatekeeper between a company's server and the outside world.



BENEFITS OF USING A FIREWALL:

1. Confidence in Choices

   There is a variety of business-class firewalls to choose from. Some network security devices include a broad range of features and services at a high cost, while others have basic services for a lower cost.

2. Functionality and Usability

   Many firewall models deliver tight security and offer GUI-friendly administration. Some of the benefits of having a GUI help prevent installation mistakes.

3. Virtual Private Network Confirmation

   A firewall purpose isn't just to keep hackers and unauthorized traffic out of the network. A good firewall also establishes and monitors secure channels and enables remote channel connectivity.

BENEFITS OF USING A FIREWALL:

4. Warranty and Technical Support

   Hardware fails. Just because a device is new and fresh from the factory doesn’t mean it will work properly.

5. Integrity of Hardware

   The hardware’s integrity is critical. Having an outdated firewall in today’s fast-paced, ever-changing business environment can lead to slowness, Internet issues, and major security concerns.

6. Monitoring and Reporting

   Firewalls manage critical network tasks. Repeatedly, throughout just one (1) business day, a single router can block thousands of intrusion attempts, detect consolidated attacks, and log failing or failed network connections.

BENEFITS OF USING A FIREWALL:

7. Content Filtering

   Is the use of a program to screen and exclude from accessing the content to Web pages or e-mail that are deemed inappropriate.

8. Failover

   Some organizations require a wide area network (WAN) failover or redundant Internet connections with automatic fault detection and correction.

9. Feature-rich

   Consider picking a firewall that has enhanced security features.

BENEFITS OF USING A FIREWALL:

10. Volume, Performance, and Capacity

Due to the network role of the firewall, this serves as an organization’s Internet gateway. Smaller offices may leverage a firewall in a dual capacity to serve as a security device and as a network switch.

11. Expertise of Installation

Installing a business class firewall properly is not as easy as it seems. Many things have to happen to set up a business-class firewall correctly

Firewall and Software

- AttackIQ FireDrill
- Bitglass
- Fidelis Deception
- GreatHorn
- JASK
- SlashNext

https://w-dog.net

BEST SECURITY SOFTWARE FOR 2019 REVIEW

ATTACKIQ

firedrill.attackiq.com

bitglass

www.bitglass.com/

Fidelis™ Cybersecurity

fidelissecurity.com

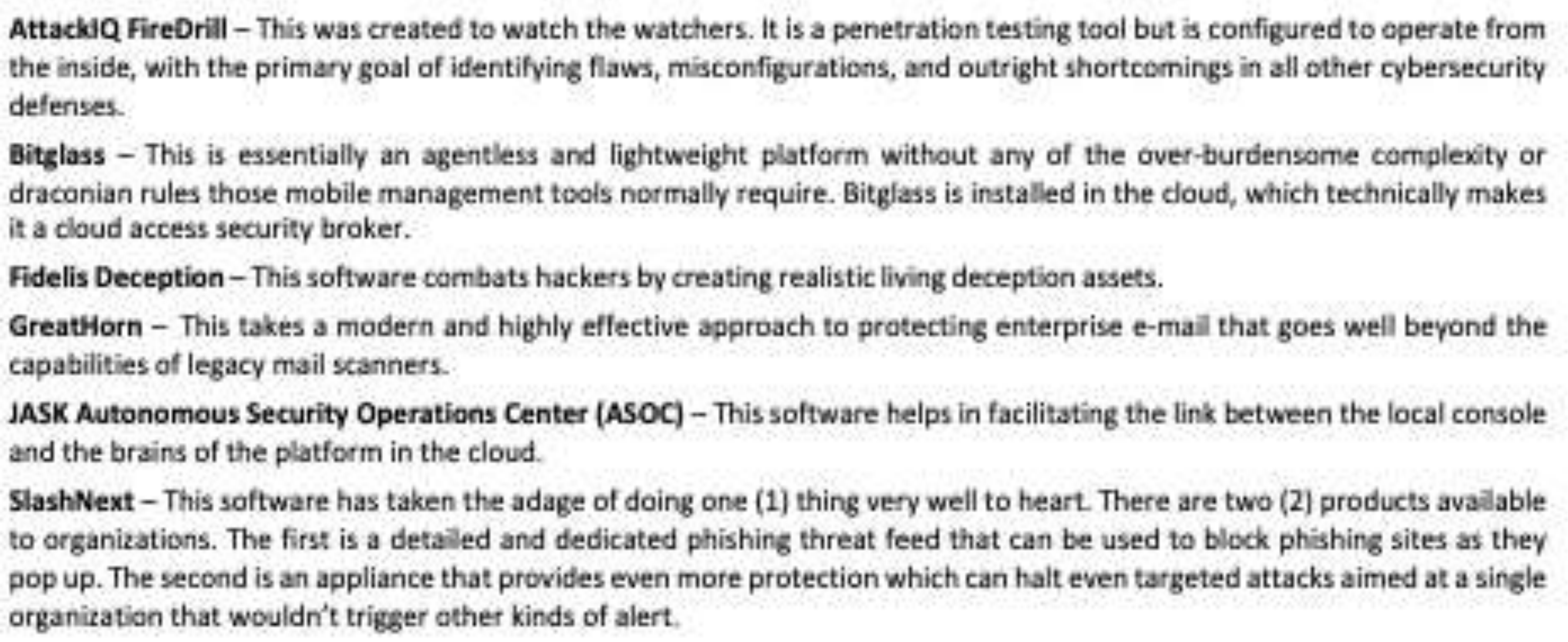
GreatHorn

www.greathorn.com/

JASK

SLASHNEXT

www.slashnext.com/



AttackIQ FireDrill – This was created to watch the watchers. It is a penetration testing tool but is configured to operate from the inside, with the primary goal of identifying flaws, misconfigurations, and outright shortcomings in all other cybersecurity defenses.

Bitglass – This is essentially an agentless and lightweight platform without any of the over-burdensome complexity or draconian rules those mobile management tools normally require. Bitglass is installed in the cloud, which technically makes it a cloud access security broker.

Fidelis Deception – This software combats hackers by creating realistic living deception assets.

GreatHorn – This takes a modern and highly effective approach to protecting enterprise e-mail that goes well beyond the capabilities of legacy mail scanners.

JASK Autonomous Security Operations Center (ASOC) – This software helps in facilitating the link between the local console and the brains of the platform in the cloud.

SlashNext – This software has taken the adage of doing one (1) thing very well to heart. There are two (2) products available to organizations. The first is a detailed and dedicated phishing threat feed that can be used to block phishing sites as they pop up. The second is an appliance that provides even more protection which can halt even targeted attacks aimed at a single organization that wouldn't trigger other kinds of alert.

AUTHENTICATION

It is a mechanism of associating an incoming request with a set of identifying credentials

TOP 6 AUTHENTICATION MECHANISM

PASSWORD

HARD TOKENS

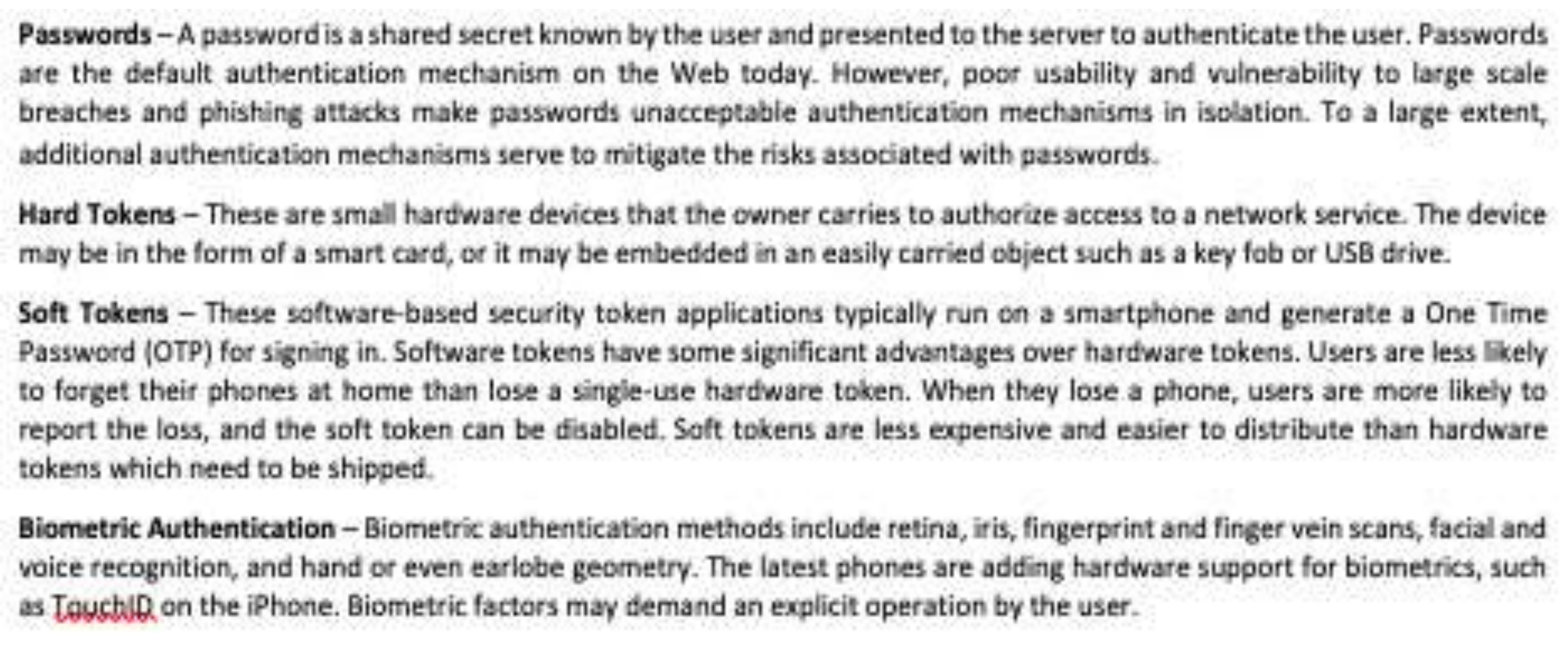
SOFT TOKENS

TOP 6 AUTHENTICATION MECHANISM

BIOMETRICS

CONTEXTUAL AUTHENTICATION

DEVICE IDENTIFICATION

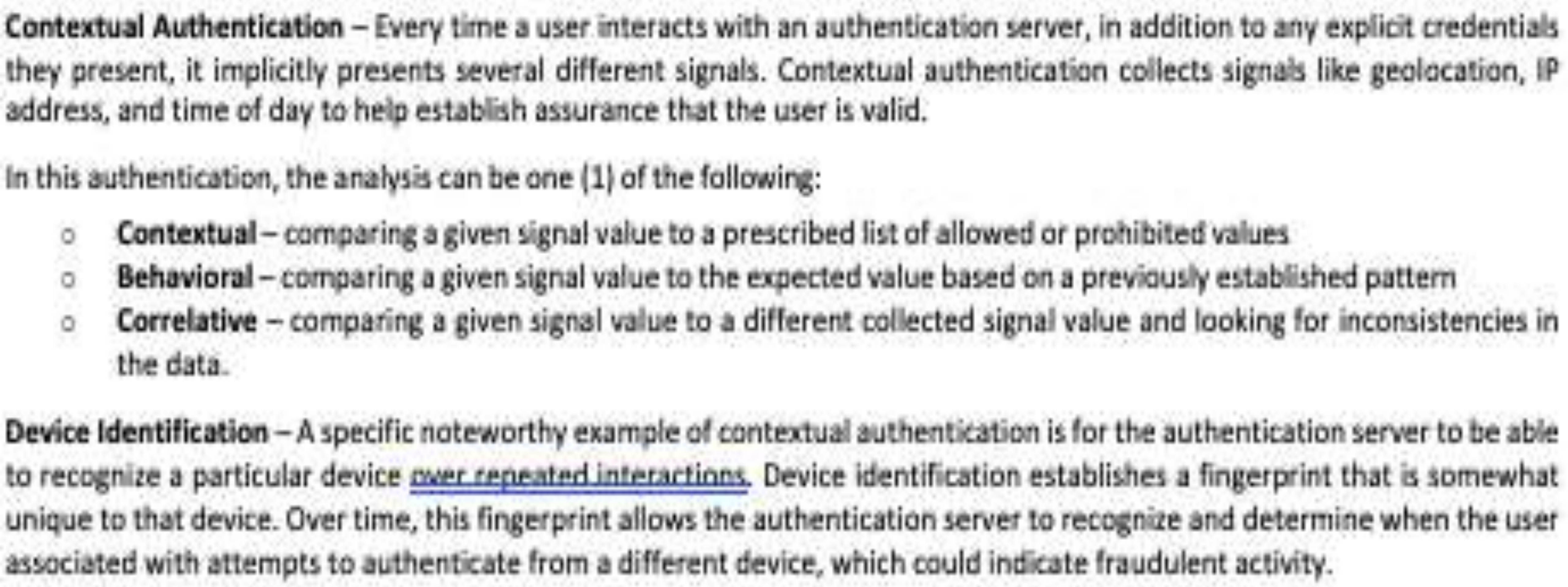


Passwords – A password is a shared secret known by the user and presented to the server to authenticate the user. Passwords are the default authentication mechanism on the Web today. However, poor usability and vulnerability to large scale breaches and phishing attacks make passwords unacceptable authentication mechanisms in isolation. To a large extent, additional authentication mechanisms serve to mitigate the risks associated with passwords.

Hard Tokens – These are small hardware devices that the owner carries to authorize access to a network service. The device may be in the form of a smart card, or it may be embedded in an easily carried object such as a key fob or USB drive.

Soft Tokens – These software-based security token applications typically run on a smartphone and generate a One Time Password (OTP) for signing in. Software tokens have some significant advantages over hardware tokens. Users are less likely to forget their phones at home than lose a single-use hardware token. When they lose a phone, users are more likely to report the loss, and the soft token can be disabled. Soft tokens are less expensive and easier to distribute than hardware tokens which need to be shipped.

Biometric Authentication – Biometric authentication methods include retina, iris, fingerprint and finger vein scans, facial and voice recognition, and hand or even earlobe geometry. The latest phones are adding hardware support for biometrics, such as TouchID on the iPhone. Biometric factors may demand an explicit operation by the user.



Contextual Authentication – Every time a user interacts with an authentication server, in addition to any explicit credentials they present, it implicitly presents several different signals. Contextual authentication collects signals like geolocation, IP address, and time of day to help establish assurance that the user is valid.

In this authentication, the analysis can be one (1) of the following:

- **Contextual** – comparing a given signal value to a prescribed list of allowed or prohibited values
- **Behavioral** – comparing a given signal value to the expected value based on a previously established pattern
- **Correlative** – comparing a given signal value to a different collected signal value and looking for inconsistencies in the data.

Device Identification – A specific noteworthy example of contextual authentication is for the authentication server to be able to recognize a particular device over repeated interactions. Device identification establishes a fingerprint that is somewhat unique to that device. Over time, this fingerprint allows the authentication server to recognize and determine when the user associated with attempts to authenticate from a different device, which could indicate fraudulent activity.