UNiTY

Connecting Everyone, Everything,
Everywhere - All The Time

Information Security for Beginners

The generic goal of most cyber-attacks is to pressure businesses and individuals to pay for encrypted or stolen data sets.

Once hackers steal login data, there is a high chance that further attacks, for example, heist sensitive information and additional phishing attacks.

Ever heard of ‘Crypto Jacking?’ this is where criminals hijack victims' computing power and mining cryptocurrency. Bitkom 2021 study showed that hackers go after the intellectual property to further cause damage to businesses of all sizes. The press release states: ‘Intellectual property like patents or research information was stolen from 18 percent – an increase of 11 percent compared to the years 2018–2019.

Typical gateways for hacker attacks:

1. Social Engineering

The human factor Social engineering is a blanket term for several malicious activities that seek to exploit every system’s greatest vulnerability: the user.

Hackers can be anyone, whether within the business with trust built or an outsider. Some hackers may build trust and relationships with employees or potentially blackmail them, to get access to important personal or business-sensitive information. Looking at cybercrime, key information that is key is passwords and credit card information. In some cases, as data is primarily digital in the current generation, hackers and criminals may pose as IT support or even people with hierarchy within an organisation, demanding that employees hand over information via email or phone. When in reality, they are giving important information over to a stranger.
If an email comes from a ‘CEO’ or someone internal asking for this type of information, it is easy to forget to check the email address or the data they have been asked for.

2. Weak Passwords

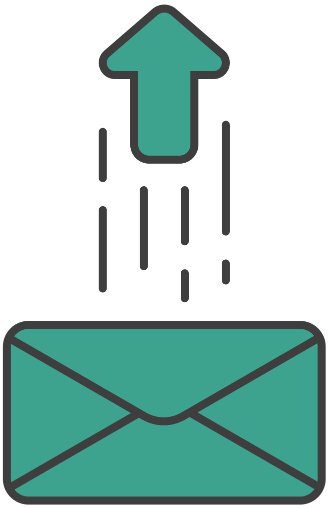
Surprisingly common passwords used could look like ‘12345678’, ‘abc12345’, ‘password1’ – these passwords potentially leave the door open easily to hackers via password spraying attacks. Whereby, hackers use software to identify passwords by entering commonly used characters and letters ‘123’ ‘abc’. Passwords that include words associated with individuals’ personal life (e.g., name of partner, pet’s name, maiden name) make it easier for cyber attackers with intimate knowledge of the individual to guess.

3. Shadow IT

Refers to hardware and software used by employees without the knowledge of the IT department.

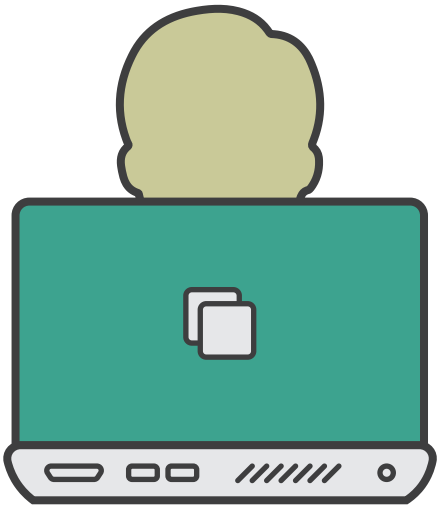
Examples include browser plug-ins and messaging clients.

As they are not part of an organisations IT system, solutions like this are more susceptible and unprotected.



4. Home Office (Remote Work)

2020 had a record-breaking amount of cyber-attacks and crimes, targeting businesses. Many businesses were ill-equipped to work from home on short notice, leaving companies heavily relying on processes and systems that were not hundred percent suitable. Over the COVID-19 period, ransomware attacks became increasingly successful for hackers. Primarily done via infected email attachments, infected downloads, and social engineering attacks.



5. Lack of Due Diligence

According to the 2019 IDG Research Services study, roughly 47% of respondents reported cyberattacks on cloud servers. With these attacks rising, it has been suggested that Cloud Service providers put businesses at risk. However, this is not always the case, the rising number of attacks is simply an expression of the increasing popularity and use of cloud services. With COVID-19 the majority of the UK began working from home, meaning Cloud services were very much in demand, due to the higher security that internally hosted IT. When choosing a cloud hosting provider, it is vital to choose the right one, as not all cloud services are created equally. Some providers have had fraught breaches concerning information security.

Before you start working with a new cloud service provider, due diligence is essential:

Is the provider's information security management system certified?

How has the service provider held up under penetration testing?

What contractual guarantees does the service provider offer?

Ensure that your SLA (Service Level Agreements) are reflecting the service your organization requires.