# CYBER SECURITY
## TOOLKIT

PREPARED BY

ARTHUR MOSES OPIO AND NSANZIMANA GILBERT

DIRECTORATE FOR ICT SUPPORT (DICTS)
MAKERERE UNIVERSITY

OCTOBER 2023

# CONTENTS

# 1. INTRODUCTION

With the advent of COVID-19, Academia wasn't spared as many had to adopt the new normal of work and study. Zoom became a household name as many meetings went virtual. Trade in Uganda took on the shape of e-commerce, it increased drastically as the likes of Jumia, Kikuubo online were embraced by many Ugandans.

E-Services and the widening use of ICT are the lifeblood of the digital economy globally. Over the last two decades, the number of e-Services globally has accelerated exponentially, helping to connect industry, facilitate trade, and drive international investment(Draft National Cybersecurity Strategy).

During the first quarter of 2021, Facebook now Metaverse stated that 3.51 billion people were using at least one of the company's core products (Facebook, WhatsApp, Instagram, or Messenger) each month (Statista).

The world we now live in is highly digital and investments in infrastructure to better services increases by the day. Many systems are connected including smart cars, smart TVs, smart watches, smart phones, etc. NITA-U has come up with a draft national cybersecurity strategy to guide Ugandans as many get to use the online space to trade, study, socialize, perform online banking, etc. With this digitization, it has huge advantages and also risks that come with it.

Globally, there were nearly 1.4 million reports of virtual identity theft in 2020 and 3.3 billion dollars was lost to fraud(Beyond Identity).

According to Beyond Identity, "Cybercrime reports have exploded in the past decade, with over 4.7 million reports in the U.S. in 2020. This represents an increase of over 300% in 2020 relative to a 2010 baseline, costing the global economy trillions of dollars in the process. "

## 1.2 INTRODUCTION

The cybercrime report of the Uganda Police acknowledged the relative increase in cases of cyber crimes related cases and they led to a loss of UGX 15,949,236,000 in 2020. It is said that the major categories of cybercrimes were electronic fraud and obtaining money by false pretense.

Uganda has enacted into law the Computer Misuse Act 2010 to enable the fight against cybercrime.

Currently the success of any organization depends upon their posture in detecting and defending against cyber attacks. A successful attack can cause effects ranging from brand reputation to shutting down of operations.

Humans are the first line of defense for every organization when it comes to cyber security. Research by IBM indicates that human error contributes 95% of all data breaches. Irrespective of the technical processes put in place to guard against cyber attacks, the human firewall must receive priority.

Employees have the capacity to determine the next stage of an organization by their behavior online.

The cyber security toolkit is developed to strengthen the human link by building awareness for a safe and secure cyberspace in Makerere University and beyond for all end users. At all costs, the human firewall must be built.

### Remember

**EVERY**

**39**

**SECS**

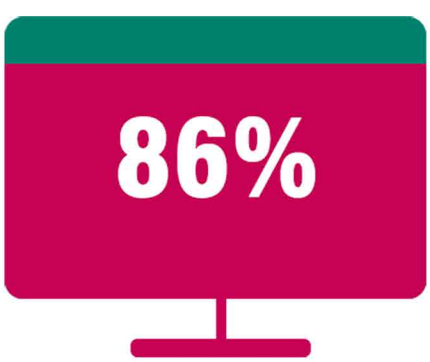
A new cyber attack takes place

# 02

# PHISHING

## What is Phishing ?

Phishing attacks are in the form of fraudulent messages that appear to come from a reputable source, usually through email. The main aim of these is to steal sensitive data such as credit card numbers, confidential corporate information and login information.




86% of all organizations had at least one person clicking a phishing link in 2021

# 2.1 HOW PHISHING HAPPENS

Email is the most common channel for phishing and accounts for 96% of all phishing attacks, according to Verizon's 2021 data breach report.

The most impersonated worldwide brands in 2021 included Microsoft, DHL, Linkedin, Amazon, Google and Paypal.

## CHANNELS OF PHISHING ATTACKS

**96%**

of phishing attacks arrive by email

**3%**

of phishing attacks are through malicious websites

**1%**

of phishing attacks using arrive through sms or calls.

## Email

Email is the most common channel for phishing and accounts for 96% of all phishing attacks, according to Verizon's 2021 data breach report.

When targeting employees or heads of organizations, common phishing subjects are "Urgent", "Request", "Important", "Payment" and "Attention"

## Malicious Websites

Attackers set up websites to collect vital information from unsuspicious users that visit them. Cybercriminals create websites that impersonate legitimate ones with a slight variation in the domain name, for example goog1e.com instead of google.com. notice in the former, a digit "1" replaced the letter "l". E-commerce websites that collect credit card details are often impersonated in this way. The attacker's site can be made to look legitimate, any data such as names, address and payment details are received by the attacker.

## Phone

It includes messages that often direct the target to visit a certain attached link. This kind of phishing is known as smishing (a combination of "sms" and "phishing").
The other form of phishing through phone is vishing in which the criminal uses a phone call claiming to be a representative of a brand well-known to the victim and asks for information that shouldn't otherwise be exposed.

## DON'T BECOME A VICTIM

While phishing attacks are rampant, short-lived, and need only a few users to take the  bait for a successful campaign, there are methods for protecting yourself. Most don't require much more than simply paying attention to the details in front of you. Keep the following in mind to avoid being phished yourself.

**3.4 B**

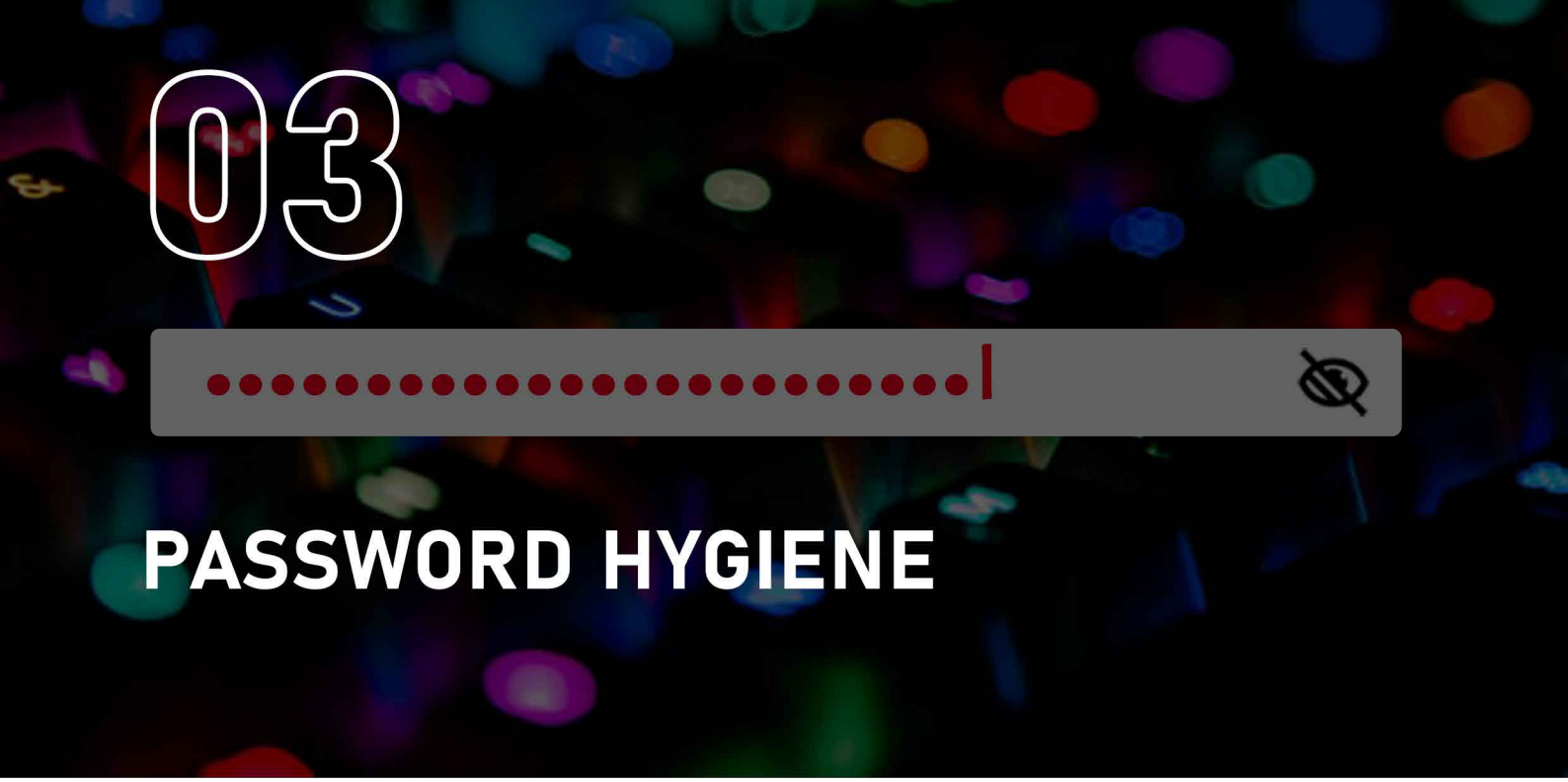
More than three billion phishing emails are sent every

**14**

An average employee receives 14 malicious emails per year

## PREVENTION TIPS

- Avoid clicking on links in unsolicited messages or emails
- Verify domain names before submitting any information
- If anything looks suspicious, do not click
- Avoid posting personal information on social media forums
- Keep your software updated
- Install and keep anti-virus software updated



# 03

# PASSWORD HYGIENE

With the hybrid workforce defined with a mixture of remote and on-site working, many employees find themselves with many passwords to memorize for different systems. In some countries, an average person is estimated to have 100 passwords and most people have 25% more passwords than at the start of the pandemic

The task is to make sure that the passwords are easy to remember and yet difficult to guess. A common tendency for many users is to focus on the ease of remembering passwords without considering their security implications.

Fear of forgetefulness is one of the reasons for poor password behavior. Reasearch conducted by Google shows that:

**59%**

use their name or birthdate in their passwords

# 3.1 PASSWORD REUSE


of people reuse passwords across multiple, if not all, sites

LastPass in its third Psychology of Passwords global report showed that 91% of people know password reuse is insecure, yet 75% do it anyway.

## Why is Password Behavior a Key Focus?

When hackers get access to one account credentials (email and password) belonging to a certain individual, the next task is to find out what other online services they use then try to login with the same compromised credentials.

In this case, it becomes a quick entry to their account if they're-used the sameSocial engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

In other common scenarios, it is a known trend for users to do a simple variation in their passwords. It's a common practice that the variation is with the date of birth, current year and some other few predictable changes.

## What to Avoid while Choosing Secure Passwords

- Avoid reusing a single password on mul-tiple accounts
- Avoid choosing passwords that contain some of your personal information

  Information such as your name, date of birth, phone number are commonly used in passwords and hackers are aware of this. Example: If a hacker knows that Peter was born in 1998, there is some tangible probability that they use peter@98 or peter@1998 as their password.

- Avoid using passwords based on letters or numbers that follow each other on the keyboard

  Passwords such as qwerty, 123456789, or 0987654321 are common and equally vulnerable to cyber attacks.

- Avoid using words that can be directly found in any dictionary.

  hackers run computer programs based on words existent in dictionaries

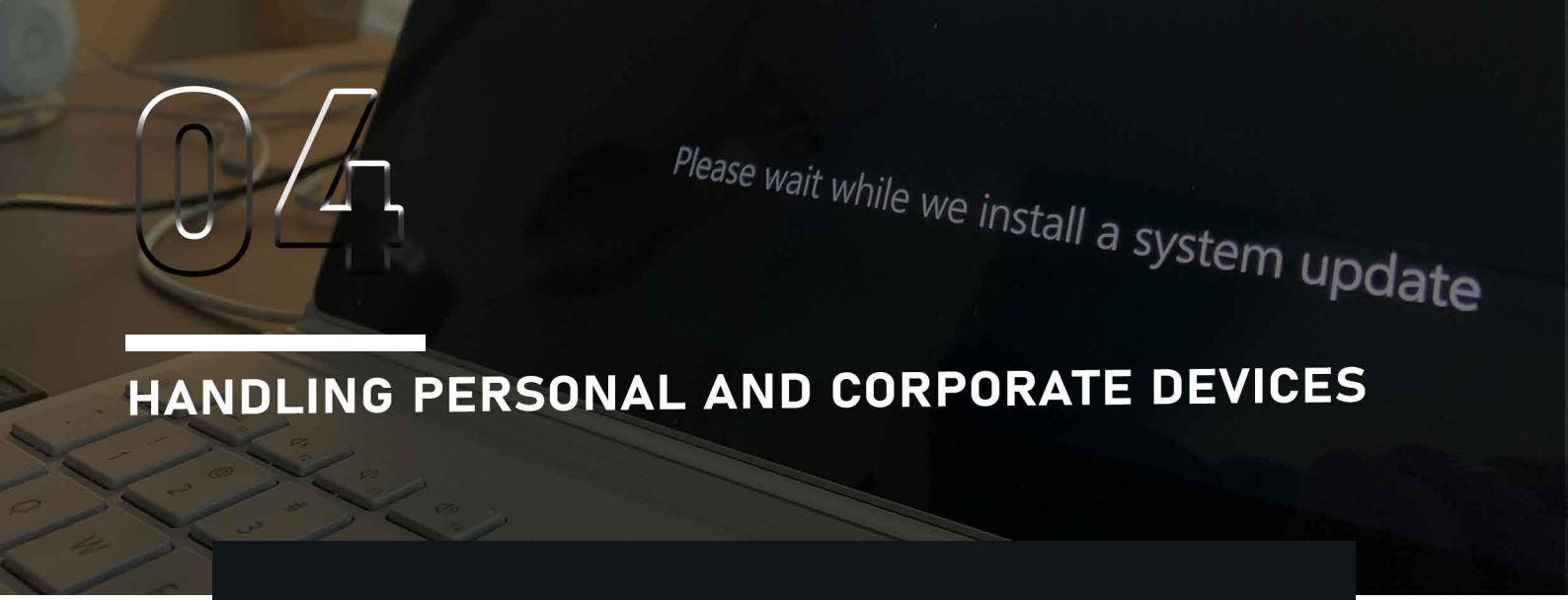
## 3.2 HINT FOR A STRONG

Using a passphrase modified at certain points is always a good idea in creating a strong and yet easy-to-remember password.

Example of a phrase used a password is “Ryseaiz#14mE”

In this particular password, the original phrase is “Rice is number one for me”. Notice how rice was written, and number 1 replaced with #1 and the rest.

Length beats complexity when it comes to password security




# 04

## HANDLING PERSONAL AND CORPORATE DEVICES

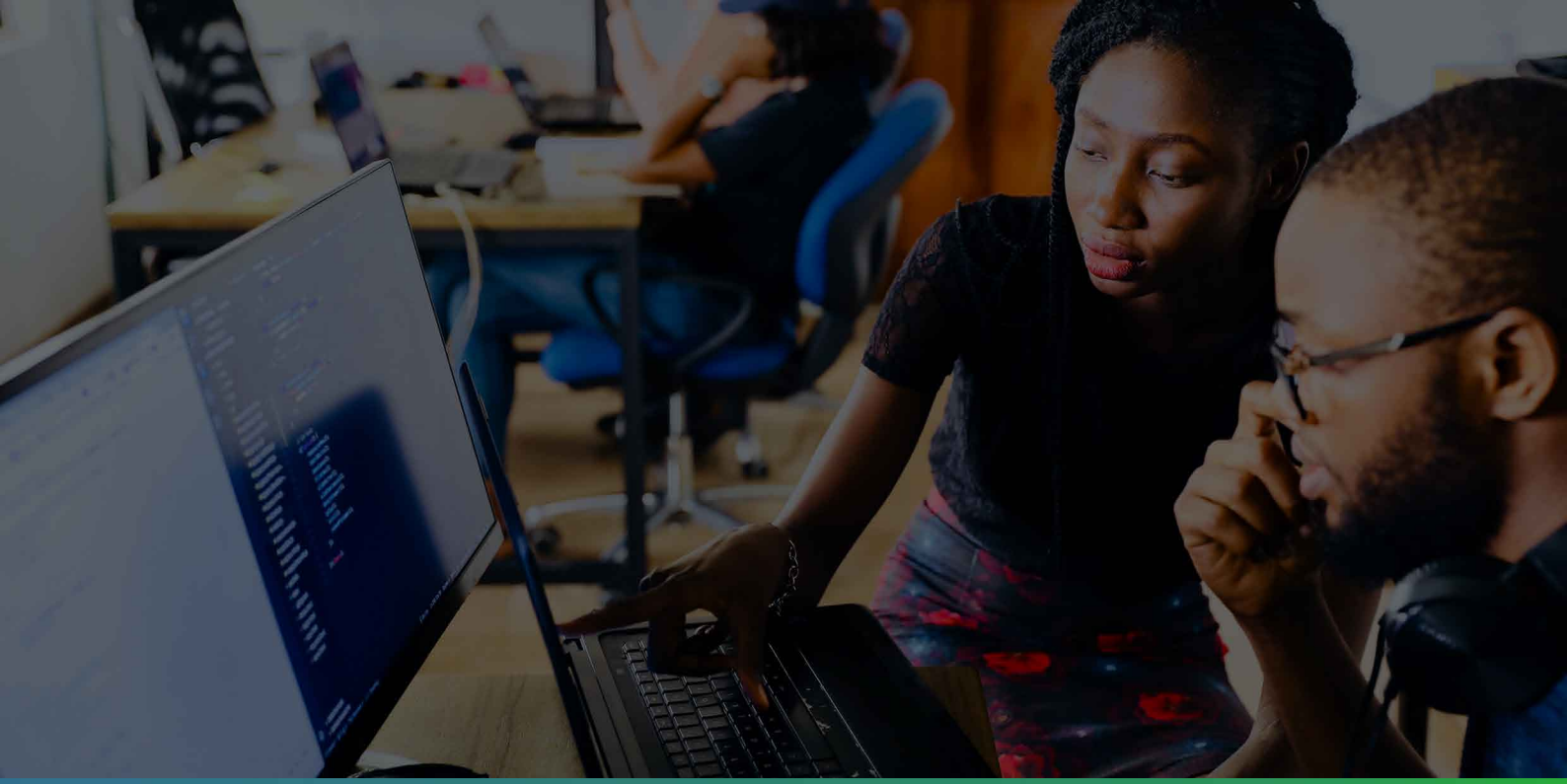
64% of all employees visit non-work related sites every day

When COVID-19 set in, companies had to adapt to the new mode of working that was majorly remote in consideration of the health safety of their workers and customers. Mobile workforces nearly doubled resulting in an overall increase in cyber attacks targeting unsuspicious users as channels corporate networks.


# 4.1 PERSONAL DEVICES

**87%** of businesses rely on their employees to use their personal mobile devices to access company apps.

Personal gadgets are targeted by hackers to "Land and expand". From a personal device, a lot of the information needed by hackers to target an organization is gathered. Information such as other workmate email addresses, a number of work-related documents, can all be used by cybercriminals to prepare and launch a cyber attack.



# 4.2 CORPORATE DEVICES

**64%**

According to Salary.com, 64% of all employees visit non-work related sites every day. Putting aside productivity concerns, employees that access websites for personal reasons can introduce malicious files or click on links that can corrupt their machine or the corporate network.

## 4.3 BEST PRACTICES TO PROTECT DEVICES

1. Enable Multi-Factor Authentication
2. Logout all your accounts when activities are complete
3. Keep all your software up-to-date
4. Share limited corporate information using a personal gadget.
5. Install and up-date security solutions such as anti-virus
6. Avoid clicking on unexpected popups

**60%**

of mobile device vulnerability derives from the client side.

**74%**

of IT leaders from global enterprises report experiencing a data breach due to a mobile security issue

# 05

# THE ETHICS OF WORKING FROM HOME

When COVID-19 came in, businesses and institutions closed their physical gates and most of the services went online. Both clients and workers are being forced to work online by the situation. Many companies lacked reliable infrastructure to facilitate the changes.

The way we work has experienced a rapid transformation since the beginning of COVID-19. As we watch for the trends in the post-pandemic workforce, here are some thoughts from workers and employers.

**73%** of employees surveyed expressed a desire for flexible remote work options post-pandemic

**66%** of businesses said they were considering redesigning physical spaces to better accommodate hybrid work environments

# SECURITY CONCERNS OF ROMOTE WORKFORCE

While working from home offers a range of benefits to workers and employers, there are several security risks associated with it. Majoly, because the security concerns are mostly on the workers' end rather than the IT staff.

Business leaders and owners tend to share a common view of being quite more vulnerable to cyber attacks when their workforce is remote.


**C-SUITES**


**SBOs**

86% of C-suites and 60% of small business owners (SBOs) believe that the risk of a data breach is higher when employees work remotely.

# WORK FROM HOME BEST PRACTICES

Cybersecurity is everyone's responsibility. The success of cybercriminals largely leverages weaknesses identified on the human layer. The following tips can help

- Install an anti-virus software
- Keep all your software up-to-date
- Enable multi factor authentication (MFA)
- Secure your Home Wi-fi
- Use company devices as much as possible
- Keep family members away from work gadgets


Your account is more than 99.9% less likely to be compromised if you use MFA


# 06

# WIFI CONNECTION SAFETY

It's a common practice to switch off personal data when there is “Free WiFi” in a spot. However users need to keep in mind that these networks are desirable to hackers as they are to users.

When asked the most common questions clients pose to coffee shop attendants, “What is your Wi-Fi password” will be mentioned among the top. For a number of employees and students, public places with ‘Free Wifi” are second to their offices.

In a certain survey conducted by Symantec, It was discovered that

**55%**

**of survey participants said they would not hesitate to connect to a free Wi-Fi hotspot if the signal was good**

# WIFI CONNECTION SECURITY RISKS

Security risks involved with connecting to unsecured public wifi hotspots span from losing personal information to hackers, through installation of malicious software on the users' devices.

Beware of the most common ways through which Wifi networks can be harmful.

## Evil Twin– Rogue Wifi Hotspots

These are Wi-fi connections setup by hackers to impersonate the legit ones available. Hackers make the hotspot names (SSID) and passwords the same as the legit ones. When a user connects to the hackers hotspot, all the data being shared can be intercepted by the hackers.

## Malware Distribution

A cybercriminal could set up a wifi hotspot with an intention to install malicious software on gadgets of those that connect to it. The malware could be viruses, ransomware, spyware and any other as intended by the hackers.

## Packet Sniffing/ Eavesdropping

By using packet sniffers, hackers can monitor web traffic through an unsecure wifi hotspot to capture personal information such as login credentials, and banking details being accessed on the network.

# BEST PRACTICES FOR WIFI CONNECTION

- Use WiFi sparingly
- Avoid using WiFi connections to access confidential information
- Keep WiFi turned OFF whenever you do not need it
- Set your Mobile phone Not to “Automatically” connect to any open WiFi
- Consider turning on VPN whenever you are using untrusted WiFi connections
- Sign out to Any WiFi connection when done

**95%**

95% of the millenials said they had shared sensitive information over open Wi-Fi connections

# REFERENCES


https://www.verizon.com/business/resources/reports/dbir/

https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe

https://www.riverbed.com/en-gb/file/survey/hybrid-work-global-survey-report-2021

https://ms-worklab.azureedge.net/files/reports/hybridWork/pdf/2021_Microsoft_WTI_Report_March.pdf

https://e2etechnologies.co.uk/blog/top-tips-on-how-to-maintain-cyber-security-when-working-from-home/

https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref

https://www.embroker.com/blog/cyber-attack-statistics/

https://www.zdnet.com/article/project-falcon-neuro-using-sensor-cameras-to-share-earth-observation-data-from-the-iss/

https://www.tessian.com/blog/phishing-statistics-2020/

https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers

https://tech.svvsd.org/blog/2021/07/21/password-reuse/

https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

https://www.techradar.com/news/most-people-have-25-more-passwords-than-at-the-start-of-the-pandemic