NAMCOR BLOG

2024

Cyber Security at Home and the Workplace

Written by:

Ndangi Nashiku

IT Security Officer & Cyber Security Expert

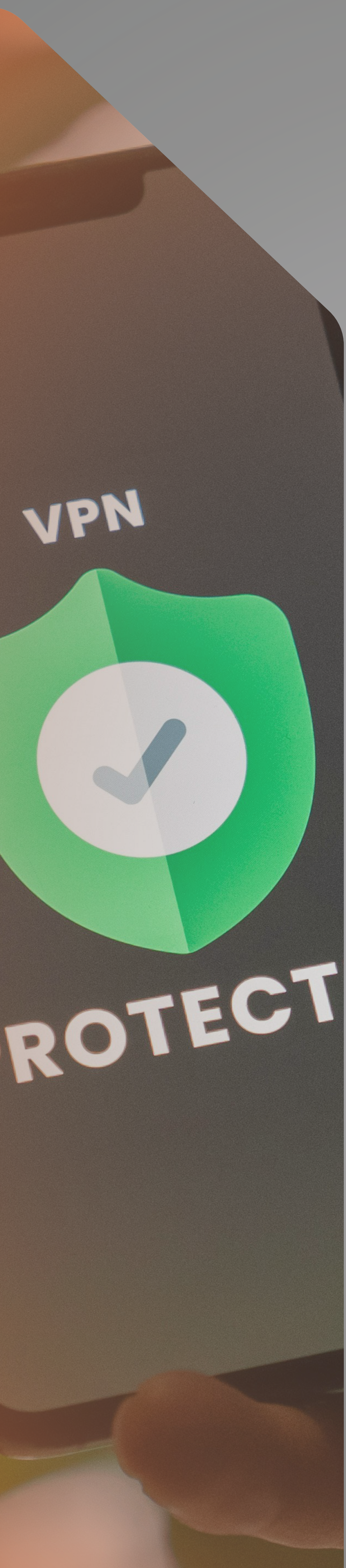
Information and Communications Technology Department

Summary

In our increasingly connected world, we rely on technology for almost everything. This convenience, however, comes with a responsibility to protect ourselves online.

Strong passwords and multi-factor authentication are essential for securing our accounts. Regularly backing up data shields us from accidental loss or attacks. By staying vigilant against phishing scams and securing our routers, we take control of our digital safety.

The same principles apply in the workplace. Educating employees on cybersecurity habits protects company data and customer information. By working together, we can create a strong defense against cyber threats.



Introduction

Our globe is now more connected than ever before thanks to the internet. With a few taps on our smartphones, we can video chat with friends all over the world, order things to arrive at our door in hours, or access massive amounts of information. We live in an era of limitless potential, with the digital frontier expanding by the day.

However, great connectedness brings immense responsibility. As our lives become more digitised and linked, we must take steps to safeguard our data and privacy. The same technology that enables us also puts us at risk if sufficient safeguards are not in place. Malicious Threat Actors (MTA's) are continually finding new methods of infiltrating unprotected devices and stealing critical data.

Password and Authentication

Passwords are the first line of defence for your digital accounts and devices. A weak, easy-to-guess password leaves you vulnerable to attack.

Enable multi-factor authentication (MFA) for an added layer of security. MFA requires providing two forms of identity verification when logging in, such as a password plus a code sent to your mobile phone. Though an extra step, MFA significantly reduces the risk of account breaches. Turn it on whenever available. With strong passwords and multi-factor authentication enabled, you can rest easy knowing your accounts and devices are protected from unauthorised access. Follow these tips for creating strong passwords.

2

Tips for your security

Use Mixed Symbols

Use a mix of uppercase and lowercase letters, numbers, and symbols. The more random, the better.

Avoid Personal Information

Avoid basing passwords on personal information, names, birthdays, or dictionary words. These are easy for Threat Actors to figure out.

Use Phrases

Opt for passphrases instead. A passphrase is a longer password made up of multiple words, like “correcthorsebatterystaple”. Easier to remember, but harder to crack!

Make Password Unique

Make every password unique. Reusing passwords across accounts is a risky practice.

Use Password Managers

Consider using a password manager like LastPass or 1Password to generate and store strong, unique passwords.

Backing Up Your Data: The Digital Safety Net

Your data is invaluable, yet a hard drive crash, ransomware attack, or accidental deletion could wipe it out in an instant. That is why regularly backing up your data is a crucial safeguard for your digital life. Here are some effective backup options to secure your files.

External Hard Drives

An external hard drive that connects via USB is one of the simplest ways to back up your data locally. Look for a drive with ample storage space - ideally double your computer's capacity. The initial backup process can be lengthy, but subsequent backups only copy newly added or changed files, making them quick and easy. Store the drive in a separate location from your computer for protection against physical calamities like fires or floods.

Cloud Storage Services

For offsite backup that keeps your data accessible from anywhere, cloud storage is ideal. Services like Google Drive, Dropbox, iCloud, and OneDrive offer ample free storage space to get started. For more storage capacity, affordable paid plans are available. Cloud backup occurs continuously and automatically if you have an internet connection. Encryption protects your data in transit and at rest. With the convenience of cloud backup, there is no excuse not to secure your data.

Antivirus: Your Digital Guardian

Antivirus software is like a shield for your devices. It scans for threats like viruses that can steal your information or lock you out.

A good antivirus program with constant updates is super important to stay safe online. It checks your files, emails, and downloads for trouble and keeps an eye on your device to catch anything bad before it happens.

Since new threats pop up all the time, updates are key to keep your antivirus on top of things. Most programs can update automatically, so you don't have to worry about it.

With a good antivirus and updates, you can enjoy the internet without worrying about your stuff getting messed with!

Avoiding Phishing Scams

Phishing frauds aim to trick you into revealing personal information or installing malware. Stay vigilant against suspicious links and deceitful messages to protect yourself. Be wary of emails, texts, social media messages, and other communications urging you to click unfamiliar links or provide alarming information designed to provoke immediate action. Hover over any link before clicking to inspect the actual destination URL. Watch for misspelled domains, odd strings of numbers/letters, or sites unrelated to the content.

If something seems suspicious, do not click. Delete the message instead. Other red flags include messages conveying a sense of urgency, promises of financial windfalls, threats of account suspension, or requests for sensitive information. Legitimate businesses will not surprise you with sudden requests via links or make threats via messages. Use common sense when evaluating communications.

If an offer seems too good to be true, or a dire warning seems overblown, you are targeted by a phishing attempt seeking personal data. Avoid opening attachments from unknown senders, which may contain malware.

When in doubt, contact the business through official channels instead of responding to messages. Your vigilance is the best defense against phishing frauds trying to steal your precious personal data or infect your devices. If a message gives you pause, that is your cue to stop and delete.

Securing Your Router: The Unsung Hero of Digital Security

In the ever-expanding digital landscape, we cannot overstate the importance of cybersecurity. As we rely more heavily on interconnected devices and cloud-based services, our home networks become the battleground for protecting our sensitive information. At the heart of this digital defense system lies the router, acting as the unsung hero – the gatekeeper that controls the flow of data between your devices and the vast expanse of the internet. Just as a well-fortified castle secures its inhabitants, a properly secured router safeguards your digital life from unauthorised access and malicious attacks. Here, we explore some best practices to ensure your router functions effectively as your digital gatekeeper:

Change Default Settings- Manufacturers often set default usernames and passwords for routers. Change these immediately to something unique and complex. Using the default credentials leaves your router vulnerable to attacks.

Update Firmware Regularly -Like software, your router’s firmware needs regular updates to patch security vulnerabilities. Check the manufacturer's website.

Why Cybersecurity in the Workplace Matters

As technology becomes more important in business, companies are at greater risk from MTA’s and data leaks. The good news is, by training employees on simple security habits, they can help protect the company's data, systems, and customers. Training helps employees avoid mistakes that can lead to cyberattacks, like falling for phishing scams or using weak passwords.

Companies also have a responsibility to protect customer information. Training everyone on cyber security helps the company follow the rules and keep information confidential.

Working together, companies and employees can build a strong defense against cyber threats. An informed workforce is the best way to stop cyberattacks.

6

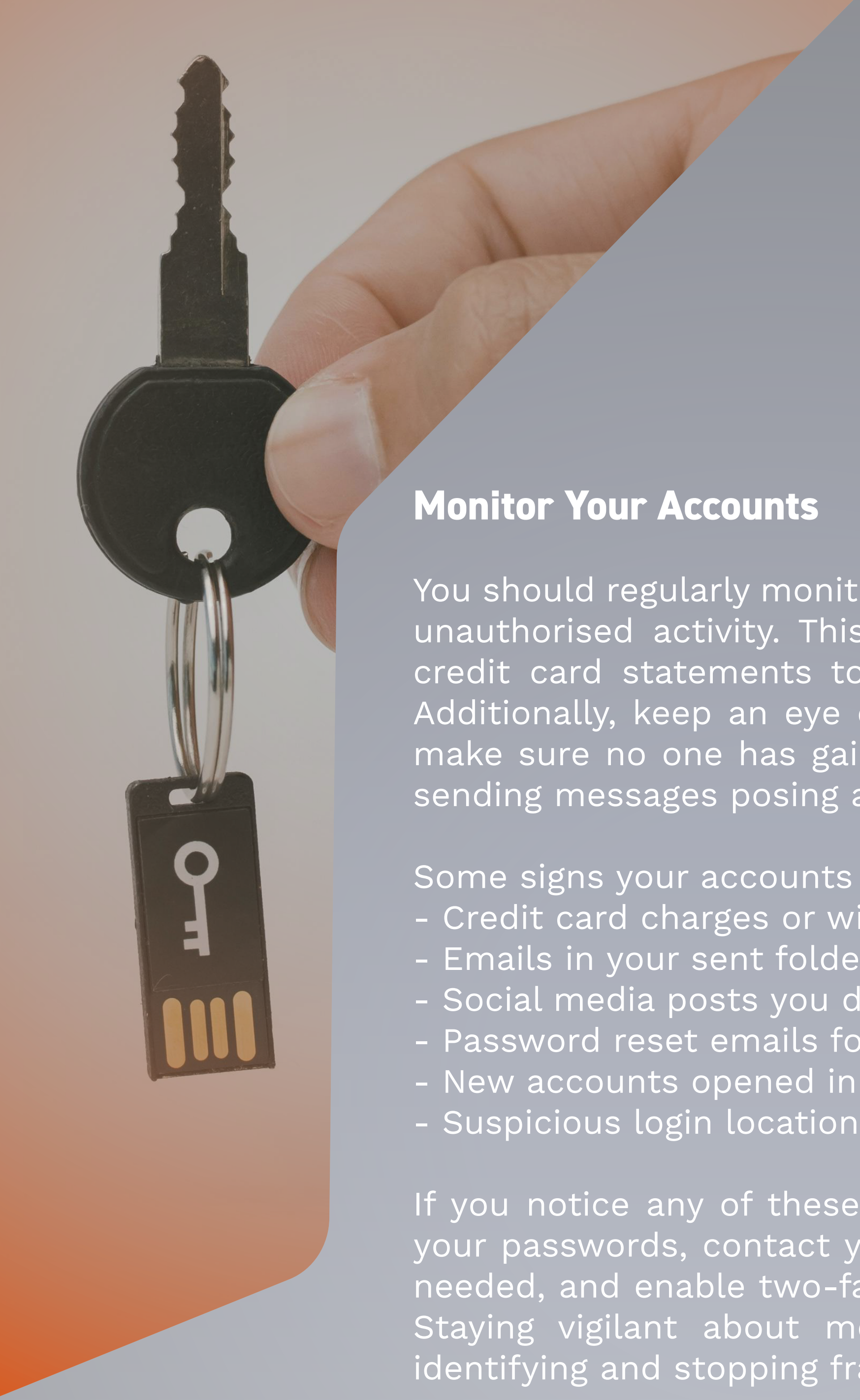
Use VPNs

Public Wi-Fi like at coffee shops isn't always safe! Someone might see your info you send online.

A VPN is like a super secure tunnel that hides your browsing, even on public Wi-Fi. Here's why you should use one:

- It keeps your online activity private.
- It scrambles your information so it can't be stolen.
- There are easy-to-use apps to connect to a VPN.

Just turn on the VPN before using public Wi-Fi and browse safely!



Monitor Your Accounts

You should regularly monitor your accounts and devices for any unauthorised activity. This includes reviewing your bank and credit card statements to ensure all charges are legitimate. Additionally, keep an eye on the sent emails in your inbox to make sure no one has gained access to your accounts and is sending messages posing as you.

Some signs your accounts may be compromised:
- Credit card charges or withdrawals you do not recognise.
- Emails in your sent folder that you did not send.
- Social media posts you did not make.
- Password reset emails for accounts you did not initiate.
- New accounts opened in your name that you did not create.
- Suspicious login locations showing up for your accounts.

If you notice any of these red flags, act immediately. Change your passwords, contact your bank, or credit card company if needed, and enable two-factor authentication where possible. Staying vigilant about monitoring your accounts is key to identifying and stopping fraudulent activity before it escalates.

Conclusion

Cyberattacks are a big threat, especially with more companies online than ever. But there's good news: training your employees on simple security habits can be your first line of defense.

By teaching them to use strong passwords, spot scams, lock devices, and use secure connections, you empower them to prevent many attacks. Regular training keeps your team up-to-date on new threats, so they can make smart security decisions. The more aware everyone is, the harder it is for MTA’s to break in.

Investing in cybersecurity training is a smart way to protect your company's data and reputation.