THE 1,2,3 OF ACCOUNT SECURITY

CYBER SECURITY AWARENESS MONTH 2020

When setting up a new account for something it's very easy to not consider the full security measures you could be taking, so we've made it as easy as 1,2,3 to set up account security! Now is a great time to review your existing accounts with the following guidance to make sure they are as secure as possible.

This is important for many reasons. Not only is a lot of personal information often stored in our accounts but our email addresses are also often used for password reset requests for other accounts. Along with our own information, our contacts are also often accessible through our accounts so protecting yourself also protects your network.

THIS GUIDE EXPLAINS HOW TO SECURE YOUR ACCOUNTS IN THREE STEPS!

1 PASSWORDS

A good, strong password should be easy for you to remember but very hard for other people to guess or for a computer to crack. Creating a strong password shouldn't be difficult. The UK National Cyber Security Centre (NCSC), recommend that you start with three well-chosen random words. For example fogautumngoat. Be sure to then include numbers, capital letters & symbols: F0g@utuMnG0@t

THE 1,2,3 OF ACCOUNT SECURITY

CYBER SECURITY AWARENESS MONTH 2020

2 REMEMBERING YOUR PASSWORDS

Having a strong, complicated and unique password for each of your online accounts is super important, but trying to remember three different random words for every different password is probably impossible! This is where writing your passwords down and passwords managers come in, and they're approaches everyone should consider.

✅ **Writing them down:** there are times when writing passwords down is the best approach to managing passwords, it's just about measuring the risk of where they're written down. It can work for many people at home, but not for people who live with those they cannot trust and absolutely not for use in an office.

✅ **Remember:** Someone is more likely to break a weak password over the internet than they are to break into your house and steal your book of passwords as a way of getting into your accounts.

✅ **Password Managers:** password managers act like a vault, you just need to remember one complicated password (make sure it's a good one!). The password manager then stores all your passwords and can help you generate new passwords for new accounts. This means you can have incredibly long, complicated passwords which offer you high levels of security. You may be wondering which one to use, some that are commonly recommended are 1Password, LastPass, Dashlane and KeePass.

3 TWO-FACTOR AUTHENTICATION / MULTI-FACTOR AUTHENTICATION

Adding an extra layer of security to your account is really important to help protect you in case your passwords get compromised. This is where two-factor authentication (2FA) and multi-factor authentication (MFA) comes in. When you set 2FA or MFA the first time you access your accounts from a different device that you don't regularly use, the website or app will prompt you to put in not just your username and password but also one (2FA) or a few (MFA) of the authentication methods listed below.

ACCOUNT SECURITY, EASY AS 1,2,3

CYBER SECURITY AWARENESS MONTH 2020

WHAT'S THE DIFFERENCE BETWEEN 2FA AND MFA?

- MFA uses two or more of the authentication methods below to access you accounts
- 2FA is a form of MFA, it uses two of the authentication methods below

Some common authentication methods along with your password include:

SMS CODE

BIO-METRICS

AUTHENTICATION APP

AUTHENTICATION PHONE CALLS

PHYSICAL TOKENS

WHAT HAPPENS IF I RECEIVE AN AUTHENTICATION CODE / CALL UNEXPECTANTLY?

If you receive an authentication code or call unexpectantly then you know your password for that account has been compromised. At this point the attacker will not have been able to access your account. However, you should go in and change the password using the password guidance above.

WHAT TO DO IF I RECEIVE A CALL OR MESSAGE ASKING FOR MY AUTHENTICATION CODE?

Never send an authentication code to anyone, for any accounts. If someone asks for your authentication code, then you know your password has been compromised. Again, at this point the attacker will not have been able to access your account. However, you should go in and change the password using the password guidance above immediately.