




# **CYBER**

## *DO'S AND DON'TS*

[KNOW MORE](#)

SEKURENET



# INTRODUCTION

CYBERSECURITY IS THE PRACTICE OF PROTECTING YOUR SYSTEMS, NETWORKS, AND DATA FROM UNAUTHORIZED ACCESS, USE, DISCLOSURE, DISRUPTION, MODIFICATION, OR DESTRUCTION.

IN TODAY'S DIGITAL WORLD, IT'S MORE IMPORTANT THAN EVER TO BE AWARE OF CYBERSECURITY THREATS AND TAKE STEPS TO PROTECT YOURSELF.

# Do's

USE STRONG PASSWORDS AND CHANGE THEM REGULARLY. A STRONG PASSWORD IS AT LEAST 12 CHARACTERS LONG AND INCLUDES A MIX OF UPPERCASE AND LOWERCASE LETTERS, NUMBERS, AND SYMBOLS. DON'T USE THE SAME PASSWORD FOR MULTIPLE ACCOUNTS. USE A PASSWORD MANAGER TO HELP YOU CREATE AND REMEMBER STRONG PASSWORDS.

ENABLE TWO-FACTOR AUTHENTICATION (2FA) WHENEVER POSSIBLE. 2FA ADDS AN EXTRA LAYER OF SECURITY BY REQUIRING A SECOND FACTOR, SUCH AS A CODE FROM YOUR PHONE, TO LOG IN TO YOUR ACCOUNTS.

BE CAREFUL ABOUT WHAT INFORMATION YOU SHARE ONLINE. DON'T SHARE PERSONAL INFORMATION, SUCH AS YOUR SOCIAL SECURITY NUMBER OR DATE OF BIRTH, ON SOCIAL MEDIA OR OTHER PUBLIC WEBSITES.

KEEP YOUR SOFTWARE UP TO DATE. SOFTWARE UPDATES OFTEN INCLUDE SECURITY PATCHES THAT FIX VULNERABILITIES THAT HACKERS CAN EXPLOIT.

BE CAUTIOUS ABOUT CLICKING ON LINKS OR OPENING ATTACHMENTS IN EMAILS FROM UNKNOWN SENDERS. PHISHING EMAILS ARE EMAILS THAT TRY TO TRICK YOU INTO CLICKING ON A MALICIOUS LINK OR OPENING AN ATTACHMENT THAT CAN INSTALL MALWARE ON YOUR COMPUTER.

BACK UP YOUR DATA REGULARLY. IN CASE OF A CYBERATTACK, YOU'LL BE GLAD YOU HAVE A BACKUP OF YOUR IMPORTANT FILES.

USE A FIREWALL AND ANTIVIRUS SOFTWARE. A FIREWALL HELPS TO BLOCK UNAUTHORIZED TRAFFIC FROM ENTERING YOUR COMPUTER NETWORK, AND ANTIVIRUS SOFTWARE CAN HELP TO DETECT AND REMOVE MALWARE.

BE AWARE OF SOCIAL ENGINEERING SCAMS. SOCIAL ENGINEERING IS A TYPE OF CYBERATTACK THAT TRIES TO TRICK YOU INTO GIVING UP PERSONAL INFORMATION OR CLICKING ON A MALICIOUS LINK.

EDUCATE YOURSELF ABOUT CYBERSECURITY. THE MORE YOU KNOW ABOUT CYBERSECURITY THREATS, THE BETTER EQUIPPED YOU WILL BE TO PROTECT YOURSELF.

# DON'TS

DON'T USE PUBLIC WI-FI FOR SENSITIVE ACTIVITIES. PUBLIC WI-FI NETWORKS ARE NOT SECURE, AND HACKERS CAN EASILY EAVESDROP ON YOUR TRAFFIC.

DON'T DOWNLOAD SOFTWARE FROM UNTRUSTED SOURCES. ONLY DOWNLOAD SOFTWARE FROM REPUTABLE WEBSITES.

DON'T CLICK ON LINKS OR OPEN ATTACHMENTS IN EMAILS FROM UNKNOWN SENDERS.

DON'T SHARE YOUR PASSWORDS WITH ANYONE.

DON'T LEAVE YOUR COMPUTER UNATTENDED WHEN YOU'RE LOGGED IN.

DON'T IGNORE SECURITY WARNINGS. IF YOUR COMPUTER OR SOFTWARE WARNS YOU ABOUT A SECURITY THREAT, DON'T IGNORE IT.

DON'T PAY RANSOMS TO CYBERCRIMINALS. IF YOU ARE THE VICTIM OF A RANSOMWARE ATTACK, DO NOT PAY THE RANSOM. THERE IS NO GUARANTEE THAT YOU WILL GET YOUR FILES BACK, AND PAYING A RANSOM ONLY ENCOURAGES CYBERCRIMINALS TO CONTINUE THEIR ATTACKS.

## **ADDITIONAL TIPS**

CONSIDER USING A VIRTUAL PRIVATE NETWORK (VPN) WHEN USING PUBLIC WI-FI. A VPN ENCRYPTS YOUR TRAFFIC, MAKING IT MORE DIFFICULT FOR HACKERS TO EAVESDROP.

BE CAREFUL ABOUT WHAT INFORMATION YOU SHARE ON SOCIAL MEDIA.

USE STRONG ENCRYPTION TO PROTECT YOUR SENSITIVE DATA.

REGULARLY REVIEW YOUR PRIVACY SETTINGS ON SOCIAL MEDIA AND OTHER ONLINE ACCOUNTS.

BY FOLLOWING THESE TIPS, YOU CAN HELP TO CREATE A MORE SECURE ONLINE ENVIRONMENT FOR EVERYONE.