1

REGULARLY UPDATE YOUR DEVICE AND SOFTWARE

"Vulnerabilities and exploits are being discovered daily. Until you apply the patches needed to prevent these they can be actively misused by an attacker. If the software allows it, turn on automatic updates in the settings."

NICOLE GASKELL

VULNERABILITY MANAGEMENT SPECIALIST, KORDIA

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

2

HOVER OVER LINKS

kordia®

"Before clicking on a link, hover your mouse over it to preview the actual URL. Ensure that it matches the legitimate website's domain and doesn't contain unusual characters or misspellings."

ELENA CALDERON
VIRTUAL SECURITY SPECIALIST, KORDIA

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

3

kordia®

BE WARY OF FINANCIAL SCAMS

"If someone calls you to offer unsolicited financial advice like pension transfers, buy-to-let investments, re-fixing your mortgage, and so on, then politely disengage and block the number. Avoid the temptation to Google the business name and visit their dodgy website, once they have planted the seed in your mind."

STEPHEN COATES

SENIOR SECURITY CONSULTANT, AURA INFORMATION SECURITY

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

kordia®

4 DONT OVERSHARE ON SOCIAL MEDIA

"Attackers can use the information you post to track you or impersonate you, leading to phishing attacks or identity theft."

KATE HAN
SECURITY CONSULTANT, AURA INFORMATION SECURITY

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

5

TRUST YOUR INSTINCTS

kordia®

"Cyber criminals and fraudsters will try to exploit your emotions to get you to do something. If an email of phone call feels out of character, if it is asking for something weird, or if you feel pressured, take time to think and confirm its legitimate. Trust your instincts."

PATRICK SHARP
GM, AURA INFORMATION SECURITY

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

6

kordia®

AI CYBER RISK

"AI chatbots are simply learning systems. They can learn information you share with them, and they can learn false or biased information. That information can be used by the AI for writing responses. Be careful with what you share, and be careful about what you believe."

PATRICK SHARP
GM, AURA INFORMATION SECURITY

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR
MORE CYBER SMART CONTENT

7

CHECK THE PADLOCK

kordia®

"Make sure the site uses HTTPS (look for the little lock icon next to the website address/URL at the top of your browser). It's not a guarantee of safety, but no lock = instant red flag."

ELENA CALDERON
VIRTUAL SECURITY SPECIALIST, KORDIA

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

8

BE WARY OF FREE CLOUD STORAGE

“We all think our information, photos, personal messages and memories are 'ours'. Using so-called 'free' cloud services may mean the company monetises your data by selling it to advertisers, research and analytics firms. Worse, some will claim ownership of your intellectual property in images, art, school essays etc.”

LYAL COLLINS
SENIOR SECURITY CONSULTANT, AURA INFORMATION SECURITY

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

9

USE MULTI-FACTOR AUTHENTICATION (MFA)

“Passwords alone are no longer enough to keep accounts safe, especially when people reuse the same password across multiple accounts. MFA provides an extra safeguard by requiring a second form of verification, such as a code sent to your phone, email, or generated by an app. This means that even if someone manages to obtain your password, they still cannot access your account.”

MATT GRAY
CYBER SECURITY SPECIALIST, KORDIA

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT

10

PHYSICALLY SECURE YOUR DEVICES

“If you’re stepping away from your computer, take a moment to lock your screen. It’s also a good idea to adjust your power and battery settings so your device locks or goes to sleep after a short period of inactivity as a failsafe. Additionally, when using laptops or mobile devices, always keep them with you in public spaces and avoid leaving them unattended.”

MATT GRAY
CYBER SECURITY SPECIALIST, KORDIA

BE CYBER SMART WITH KORDIA

SCAN THE CODE FOR MORE CYBER SMART CONTENT