Robert Morris University

6001 University Boulevard
Moon Township, PA
15108-1189

412-397-3000

RMU.EDU

Cybersecurity Awareness Materials
Email to all plus attachments which were displayed as posters around campus

RMU Technology Notice
Happy Cybersecurity Awareness Month!

Important: Robert Morris University Information Technology will **never** ask you to provide sensitive information including passwords.

Happy Cybersecurity Awareness Month!

Greetings,

October is Cybersecurity Awareness Month. Throughout the month we will be sending tips and awareness content to help you better secure your personal and work computing environments and data. This content will include video training, the first of which will be sent out later today. This content is optional, but we highly encourage you to watch these brief videos. Later in the month we will be holding a contest with prizes, you must have watched the training videos in order to be eligible to win.

Please find attached two cybersecurity tip sheets.

Clean Desk Best Practices

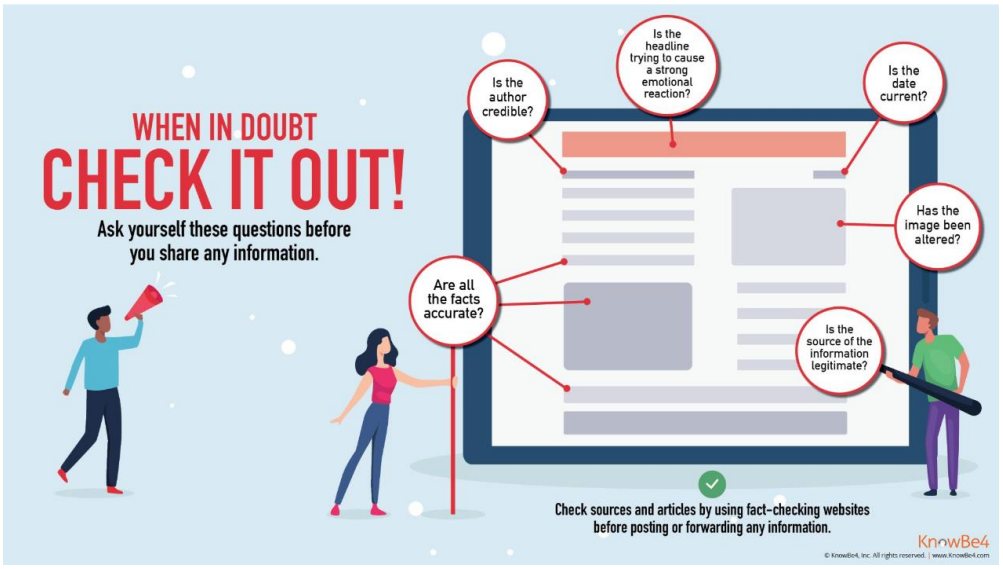
20 Ways To Build Your Security Fortress From Anywhere

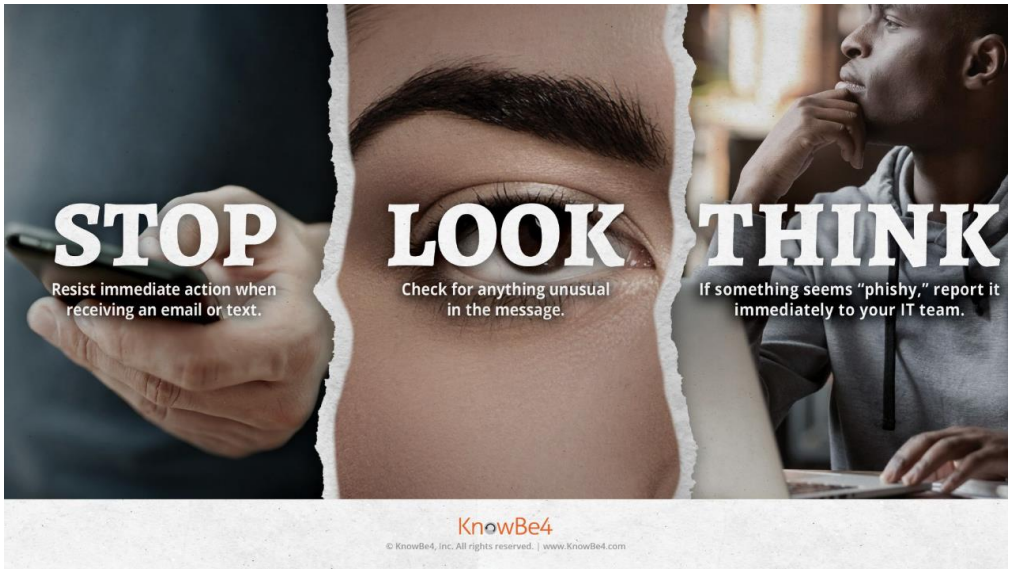
We use a third party provider, KnowBe4, for cybersecurity training and Phishing exercises. The training videos will come into your inbox from knowbe4.com and it can be trusted.

Robert Morris University
Information Technology
Help Desk
412-397-2211
help@rmu.edu

Did you know?

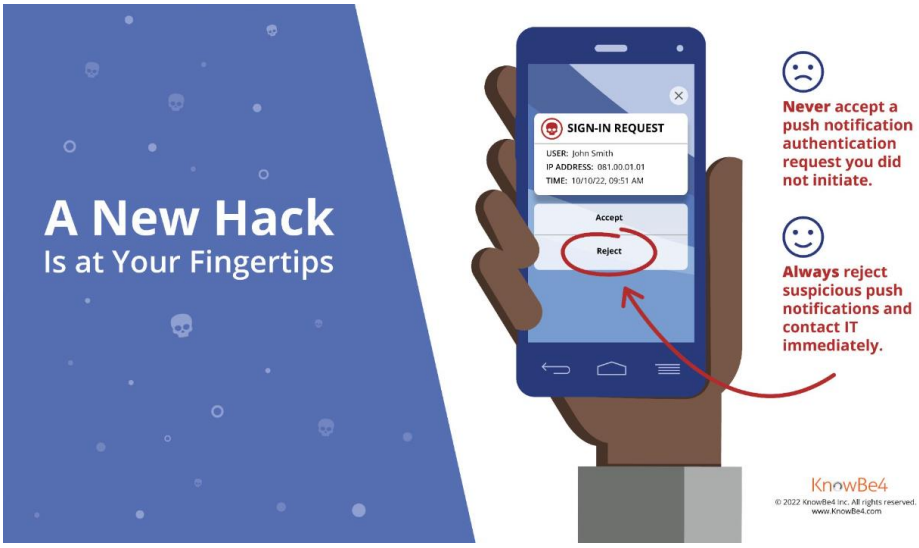
- You can reactivate your account by going to www.rmu.edu/reactivate.
- You can reset your RMU passwords by going to www.rmu.edu/password.


WHEN IN DOUBT
CHECK IT OUT!
Ask yourself these questions before you share any information.
Is the author credible?
Is the headline trying to cause a strong emotional reaction?
Is the date current?
Has the image been altered?
Are all the facts accurate?
Is the source of the information legitimate?
Check sources and articles by using fact-checking websites before posting or forwarding any information.
KnowBe4
© KnowBe4, Inc. All rights reserved. | www.KnowBe4.com


STOP
Resist immediate action when receiving an email or text.
LOOK
Check for anything unusual in the message.
THINK
If something seems "phishy," report it immediately to your IT team.
KnowBe4
© KnowBe4, Inc. All rights reserved. | www.KnowBe4.com


Don't Make Yourself a
TARGET!
Be careful what you post on social media.
KnowBe4
© KnowBe4, Inc. All rights reserved. | www.KnowBe4.com


RESIST THE
USB ATTACK
KnowBe4
Human error. Conquered.
Don't *plug* it in… Turn it in!
If you find a USB drive,
please drop it off at the IT Help Desk Hale 205


A New Hack
Is at Your Fingertips
SIGN-IN REQUEST
USER: John Smith
IP ADDRESS: 081.00.01.01
TIME: 10/10/22, 09:51 AM
Accept
Reject
Never accept a push notification authentication request you did not initiate.
Always reject suspicious push notifications and contact IT immediately.
KnowBe4
© 2022 KnowBe4 Inc. All rights reserved.
www.KnowBe4.com


THINK Before You SCAN
It's impossible to know where a QR code
will take you before scanning it.
Always check for physical tampering.
When in doubt, don't scan!
KnowBe4
© 2023 KnowBe4, Inc. All rights reserved. | www.KnowBe4.com


20 WAYS TO BUILD YOUR SECURITY FORTRESS FROM ANYWHERE
AT HOME
❑ Have separate devices for work and personal use
❑ Connect to Ethernet (wired) or at least WPA2 (Wi-Fi Protected Access 2) for a secure wireless connection
❑ Use a VPN (Virtual Private Network) whenever possible to access employer systems/data
❑ Keep router and modem firmware up-to-date
❑ Secure IoT devices (smart speakers, appliances, etc.) - use strong, unique passwords whenever possible
CLOUD SECURITY REMINDERS
❑ Enable multi-factor authentication (MFA) that requires a separate device when possible
❑ Practice good password hygiene
❑ Never save passwords in your browser
❑ Keep work-related communication to systems approved by your organization
❑ Check privacy/location/security settings on apps and restrict any unnecessary access
TRAVELING
❑ Don't use public Wi-Fi when accessing confidential info, use a personal hotspot instead
❑ Keep devices secure and accounted for at all times
❑ Disable automatic bluetooth pairing
❑ Don't allow your devices to auto-join unfamiliar Wi-Fi networks
❑ Don't use borrowed chargers or public charging stations
PHYSICAL SECURITY REMINDERS
❑ Never use unknown USB devices
❑ Always lock your workstation
❑ Keep confidential information secure - use privacy screens and headphones if necessary
❑ Implement a clean desk policy by removing business documents, notes, etc.
❑ Don't allow unauthorized individuals to tailgate
KnowBe4
Human error. Conquered.
SECURITY AWARENESS TRAINING | www.KNOWBE4.com
© 2020 KnowBe4, Inc. All rights reserved.


CLEAN DESK BEST PRACTICES
What's wrong in this picture?
Google


CLEAN DESK BEST PRACTICES
What's wrong in this picture?
1. Office door is open, office is unattended
2. Computer is unlocked and unattended
3. Password left on a sticky note
4. USB drive left out in the open
5. Keys left unattended
6. Documents left unattended
7. Wallet left unattended
8. Phone left unlocked and unattended
Google

RMU Technology Security Alert/Action Required
Smishing | Beware of Fraudulent Text Messages

Important: Robert Morris University Information Technology will **never** ask you to provide sensitive information including passwords.

Smishing | Beware of Fraudulent Text Messages

A social engineering attack, called Smishing, is being conducted right now against RMU employees and students. Smishing occurs when a cybercriminal poses as someone we know, a government agency, or another authority figure and uses mobile text messages to try to trick us into sending money to the criminal, downloading malware, or sharing sensitive information.

In recent attacks, the criminal posed as President Michelle Patrick, asking for gift cards to be purchased and shared with her.

RMU employees will never use text messages or email to ask you to purchase gift cards or send money to them. If you receive a suspicious message, please do not reply and notify the Help Desk immediately at help@rmu.edu or 412-397-2211.

Robert Morris University
Information Technology
Help Desk
412-397-2211
help@rmu.edu

Did you know?

- You can reactivate your account by going to www.rmu.edu/reactivate.
- You can reset your RMU passwords by going to www.rmu.edu/password.