CYBER TIPS 4 YOU
网络安全贴士

Protect yourself from cyber threats and online scams by practising four Cyber Tips.

采用四个网络安全贴士，保护您免受网络威胁。

BE CYBER SAFE
做好防范，安心上网

Beware of Phishing Scams
小心网络钓鱼骗局

- Think before you click on links provided in unsolicited emails and text messages.
- Always check the authenticity of the email, call or request through official sources.
- Only download apps from official apps stores, such as Google Play Store (Android) or Apple App Store (iOS).

- 不要点击未经请求的电邮及短信中提供的网络链接。
- 请通过官方网站核实电邮、电话或请求的真实性或来源。
- 只从官方应用商店如谷歌或苹果应用商店下载应用程序。

Enable 2FA and Use Strong Passphrases
启用双重认证功能(2FA)并使用安全性高的密码短语

Enable Two-Factor Authentication (2FA) where available and use strong passphrases to keep your online accounts and personal information safe.

Create strong passphrases that are easy to remember by:

- Stringing together five different words, comprising at least 12 characters, that relate to a memory unique to you, e.g. Ihadkayatoastat8am
- Using uppercase and lowercase letters, numbers or symbols to make it stronger, i.e. IhadKAYAtoastAT8AM!

尽可能开启双重认证（2FA），并使用安全性高的密码短语确保账户和个人资料的安全。

如何设置安全性高的个人化密码：

- 密码短语的设定尽量个人化，至少包含12个字符并且将五个不同的单词连起来。
- 使用大小写字母、号码和符号组成来增加密码强度。

Update Your Software Promptly
及时更新您的软件

Software and app updates contain important security fixes that can help keep your devices safe from cybercriminals.

If your software and apps are not up to date, cybercriminals could use these vulnerabilities to infect your devices with malware, steal your data and even take control of your devices.

软件和应用程序更新包含重要的安全修复，有助于保护您的电子设备免受网络罪犯的侵害。

如果您的软件和应用程序不及时更新，网络罪犯就可能利用这些漏洞在您的电子设备安装恶意软件，窃取您的个人资料，甚至控制您的电子设备。

Get more cyber tips at:
安全贴士请扫描二维码：

Add ScamShield and Anti-Virus Apps
添加 ScamShield 应用并设置反病毒（Anti-Virus）应用程序

Cybercriminals often target victims through SMSes or phone calls. Do add the ScamShield app which can protect you by detecting scam messages and blocking scam calls.

Anti-virus apps can detect malware and malicious phishing links which help safeguard your devices and accounts.

网络罪犯通常会通过短信或电话锁定受害者。您能通过下载防诈应用ScamShield以屏蔽诈骗号码减少收到诈骗短信和电话。

反病毒应用程序可以检测恶意软件和钓鱼活动，有助于保护您的电子设备和账户。

Better cyber safe than sorry

CSA SINGAPORE
Cyber Security Agency of Singapore

www.csa.gov.sg

WHAT ARE THE ONLINE DANGERS?
我们面临怎样的网络风险?

PHISHING is a method which cybercriminals use to trick victims into giving out personal and financial information such as passwords, One-Time Passwords (OTPs) or bank account numbers. Cybercriminals may impersonate organisations such as the government or banks and contact you.

网络钓鱼是网络罪犯使用的一种手法，目的是诱使受害者提供个人和财务信息，如密码、一次性密码 (OTP) 或银行账户号码。 网络罪犯可能冒充政府或银行等组织联系您。

MALWARE is a type of software that infects your devices and causes damage, including stealing your information, corrupting and even deleting your data. Once downloaded, cybercriminals can gain access to your devices, retrieve your banking credentials and make withdrawals from your bank accounts.

恶意软件是一种入侵您的电子设备并造成损害的软件，这包括窃取个人资料，破坏甚至删除个人数据。一旦下载，网络罪犯就可以入侵您的设备，检索您的银行凭据，并从您的银行账户中取款。

OUR DIGITAL USAGE
我们的数字使用

The increased use of smartphones and other digital tools has made life more convenient. Communication apps help us stay in touch with friends and family, government services & lifestyle apps bring us convenience, while e-payments & digital banking apps facilitate online transactions. However, as we go online more often to carry out these tasks, we are also more exposed to cyber threats such as online scams and data theft.

随着智能手机和电子设备的使用变得普遍化，我们的生活也变得更加便利。通讯应用程序帮助我们与朋友和家人保持联系，政府服务和生活方式应用程序为我们带来方便，而电子支付和数字银行应用程序则促进了网上交易。 然而，随着我们更频密地上网，我们也更容易受到网络威胁，如网络诈骗和数据盗窃。

Pause to check and call a family member or friend for advice.
If unsure, call the Anti-Scam Hotline at 1800-722-6688.

请暂停并检查，以及询问家人或朋友的意见。
如果不确定，请拨打反诈骗热线 1800–722–6688。

DIGITAL BANKING

Digital Banking Scams

Cybercriminals pretend to be from the bank, asking you to follow urgent instructions to address some bank account or technical issues, or provide personal information for an offer that may not exist. They may do so through text messages, emails, phishing websites or phone calls to trick you into giving away your login credentials and One-Time Password (OTP).

+65 0123 4567

Text Message
Today 3:29 PM

XYZ BANK
PayNow! :
A payment was attempted from a NEW DEVICE.
If this was NOT you, please visit http://pay-nowone.life/.

Be Cyber Safe Checklist

- ✓ Enable Two-Factor Authentication (2FA) where available and use strong passphrases.
- ✓ Set up bank transaction alerts by setting up email or SMS notifications to help you keep track of transactions.
- ✓ Report to your bank if you suspect that your account has been compromised. Lodge a police report if there is monetary loss.

- ✖ Do not contact the organisation via the contact details provided in the call or message. Verify suspicious calls or messages by calling the official hotline or checking official app/website directly.
- ✖ Never share your password, OTP or personal and banking information with unverified sources.
- ✖ Do not panic. Call your family members or friends or call the Anti-Scam helpline at 1800-722-6688 for advice.

网络银行

网络银行骗局

网络罪犯谎称是银行员工，要求您遵循紧急指示，解决一些银行账户或技术问题，或为一个不存在的优惠作为诱饵要求您提供个人信息。 他们可能会通过短信、电子邮件、钓鱼网站或电话等方式诱骗您提供登录凭证和一次性密码 (OTP)。

+65 0123 4567

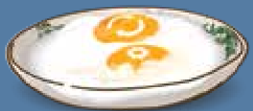
Text Message
Today 3:29 PM

XYZ BANK
PayNow! :
A payment was attempted from a NEW DEVICE.
If this was NOT you, please visit http://pay-nowone.life/.

网络安全核对表

- ✓ 尽可能开启双重认证 (2FA)，并使用安全性高的密码短语。
- ✓ 设定银行交易提示的电子邮件或短信通知来核查所属账户是否有未经授权的交易。
- ✓ 如果怀疑自己的账户被盗，请向银行报告。如果涉及金额损失，请向警方报案。

- ✖ 不要通过电话或信息中提供的联系方式与该组织联系。应直接拨打政府/企业的官方热线或查询官方应用程序/网站来验证可疑的电话或信息。
- ✖ 不要将您的密码、OTP 或个人信息和银行信息透露给未经验证的来源。
- ✖ 不要惊慌。如果不确定，您可致电给家人或朋友，或拨打反诈骗热线 1800–722–6688 寻求协助。



您知道吗？银行不再通过电子邮件或短信中发送可点击链接。

E-COMMERCE

E-Commerce Scams

Cybercriminals use attractive discounts and offers, to lure you into making purchases and insist on immediate payment or bank transfers before delivery.

They may also trick you into clicking on links or scanning QR codes which will lead you to websites requiring you to fill in your personal information. They may also ask you to download malicious apps which will allow them to access your devices, steal your banking credentials and withdraw money from your accounts.

Be Cyber Safe Checklist

- ✓ Purchase only from reputable sites. Always go to the store's official website to see if the deals are valid.
- ✓ Only download apps from official platforms, such as Google Play Store (Android) or Apple App Store (iOS).
- ✓ Use only official e-payment apps (e.g. DBS PayLah!, GrabPay).

- ✗ Do not scan QR codes in the form of stickers or flyers placed randomly in public places. Verify them with authorities and business owners.
- ✗ Never download or grant access to unknown apps as this may give cybercriminals access to your devices and accounts.
- ✗ Do not share personal or financial information unless you are sure it is a legitimate request.

Beware of Phishing Scams. If the deal is too good to be true – think again!

电子商务

电子商务骗局

网络罪犯会利用诱人折扣和各种令人难以置信的优惠，网络罪犯会坚持要求在交货前先付款或银行转账。

他们还可能诱骗您点击链接或扫描二维码，从而进入另一个网站，要求您填写个人信息。他们也可能会叫您下载恶意应用程序，从而入侵您的电子设备、窃取您的银行凭证并从您的账户中取款。

网络安全核对表

- ✓ 只从信誉良好的网站购买商品。请通过商家的官方网站查看这些优惠有没有效。
- ✓ 只从官方应用程序商店如谷歌或苹果应用商店下载应用程序。
- ✓ 只使用官方的电子支付应用程序(如 DBS PayLah!、GrabPay)。

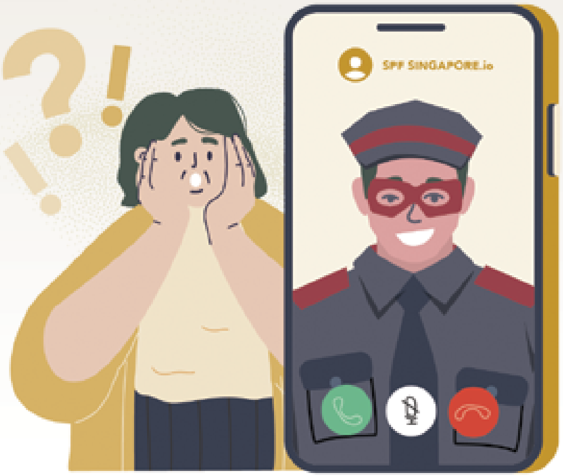
- ✗ 不要扫描公共场所随意放置的贴纸或传单形式的二维码。向相关部门和企业主核实。
- ✗ 切勿下载或授予未知应用权限，因为这可能会让网络罪犯入侵您的电子设备和账户。
- ✗ 除非能确定是合法的要求，否则不要透露任何个人或财务信息。

小心网络钓鱼骗局。如果优惠好得难以置信，请务必三思。

GOVERNMENT SERVICES

Government Impersonation Scams

Cybercriminals pretend to be from government organisations in emails, text messages or phone calls, asking you for personal information or to download malicious apps to steal your money. For example, they may claim to be an officer from CSA or the Police, investigating suspicious activity on your network, and ask for your personal information.



Be Cyber Safe Checklist

✓ Enable Two-Factor Authentication (2FA) where available and use strong passphrases.

✓ Government officials will never demand immediate payment online or instruct you to transfer money to any local or foreign bank account or disallow you from hanging up a call.

✗ Never share your password, One-Time Password (OTP) or personal and banking information with unverified sources.

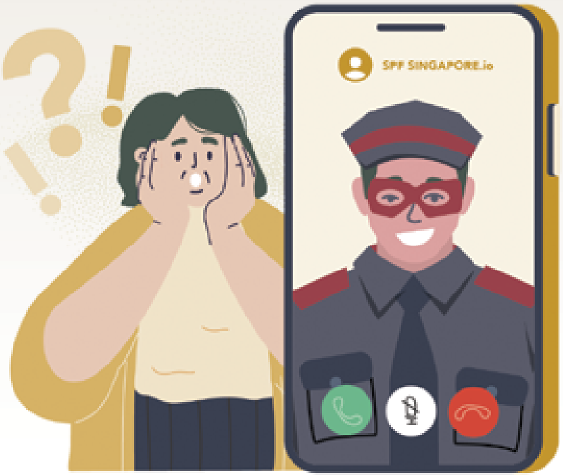
✗ Do not panic. Call your family members or friends or call the Anti-Scam helpline at 1800-722-6688 for advice.

Refer to the list of trusted government-related websites at www.gov.sg/trusted-sites if the link or email address does not have ".gov.sg" in them.

政府服务

冒充政府骗局

网络罪犯冒充政府部门，通过电子邮件、短信或电话向您索要个人信息或要求您下载恶意应用程序以盗取您的钱财。例如，他们可能声称自己是网络安全局、警方或电信公司的工作人员，正在调查您网络上的可疑活动，并要求您提供个人信息。



网络安全核对表

✓ 尽可能启动双重认证功能 (2FA)， 并使用安全性高的密码短语。

✓ 政府官员绝不会要求您立即在网上付款，或指示您把钱转到任何本地或外国银行账户，或不允许您挂断电话。

✗ 切勿将您的密码、一次性密码 (OTP) 或个人信息和银行信息透露给未经验证的来源。

✗ 不要惊慌。如果不确定，您可致电给家人或朋友，或拨打反诈骗热线 1800–722–6688 寻求协助。

如果链接或电子邮件地址中没有“.gov.sg”，请参考 www.gov.sg/trusted-sites 的可靠政府相关网站列表。

E-PAYMENT

E-payment Scams

Electronic payments (E-payments) are simple and secure digital transactions. Such services have changed the way we transact and have increasingly become a vital mode of receiving payment for business owners. However, cybercriminals can physically tamper with the QR code of your business, resulting in customers making payment directly to the cybercriminal or leading them to websites designed to scam customers of their personal information.

Cybercriminals may also contact you through text or calls, claiming to be a government authority or bank to "check" on issues related to your business and ask for your personal information or request for payment of a business-related fine.

Be Cyber Safe Checklist

✓ Verify suspicious calls or messages by calling government/banks' official hotline or contacting them via the official app/website.

✓ Only download banking apps from official platforms such as Google Play Store (Android) or Apple App Store (iOS) and set up bank transaction alerts by setting up email or SMS notifications to help you keep track of transactions.

✗ Do not forget to update your software and apps promptly as cybercriminals can make use of vulnerabilities to infect your devices with malware and steal your data and/or funds.

✗ Do not panic. If you face issues with payments using SGQR or suspect fraud, report this to the financial institution that you use to process your payment transactions from your customers.

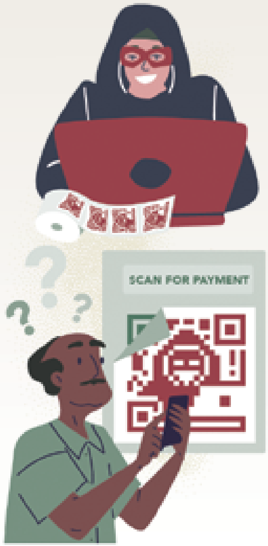
QR codes are not dangerous but cybercriminals with malicious intentions could make use of QR codes to redirect users to a phishing website or initiate a download that contains malware.

电子支付

电子支付骗局

电子支付（E–payment）是一种简单和安全的数字交易。数码服务改变了我们的交易方式，并成为企业主要收款的重要方式。然而，网络罪犯可能会篡改您企业所用的二维码，导致客户直接向网络罪犯付款，或将客户引向有意骗取客户个人信息的网站。

网络罪犯还可能通过短信或电话与您联系，声称自己来自政府部门或银行，要“审查”与您的业务相关的问题，并要求您提供个人信息或支付与业务相关的罚款。



网络安全核对表

✓ 通过直接拨打政府/企业的官方热线或查询官方应用程序/网站来验证可疑的电话或信息。

✓ 只从官方应用程序商店如谷歌或苹果应用商店下载应用程序并且设定银行交易提示的电子邮件或短信通知来核查银行交易。

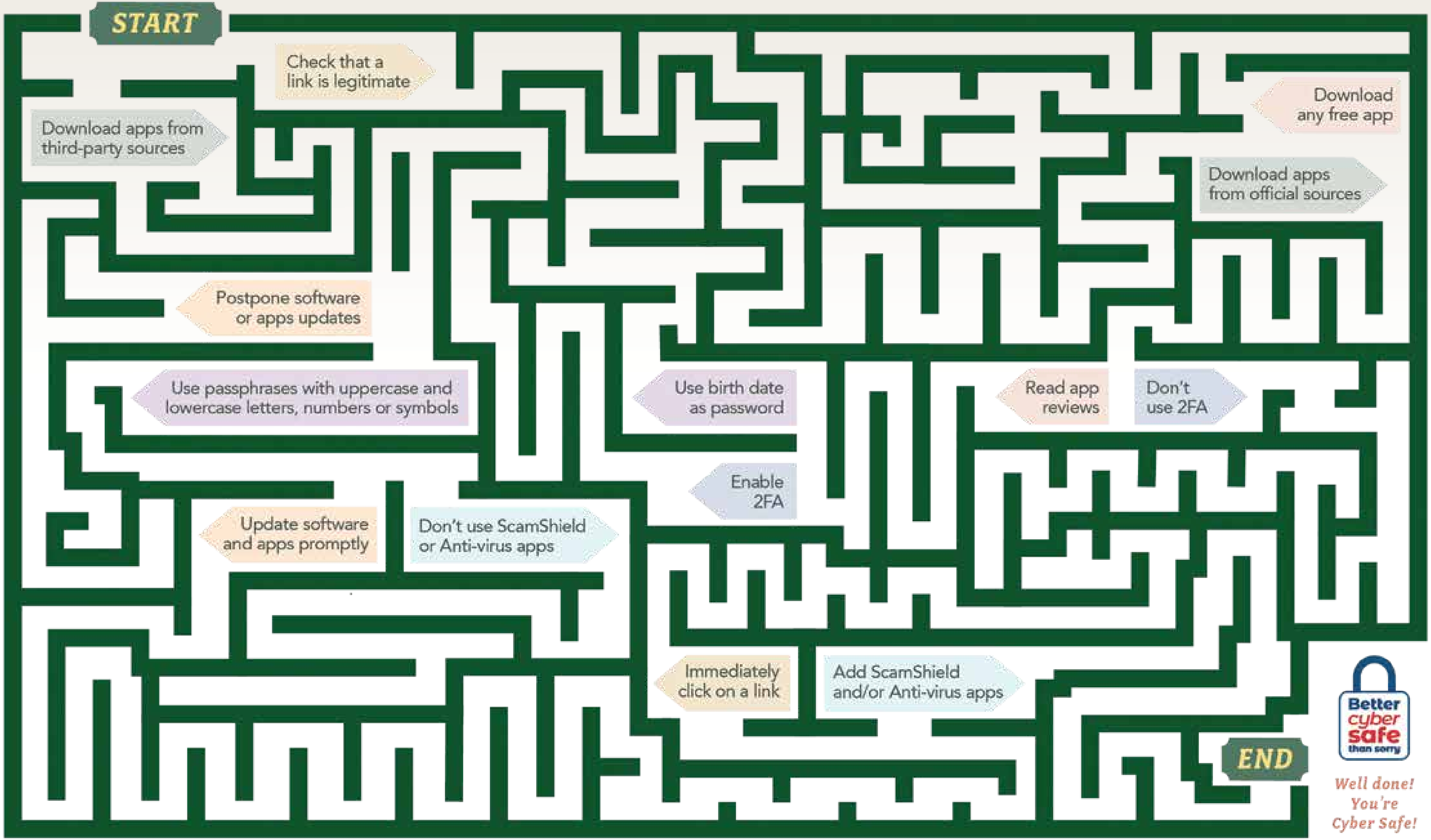
✗ 请记得及时更新软件和应用程序. 网络罪犯会利用电子设备的安全漏洞，使用恶意软件感染您的电子设备，并窃取您的个人资料和/或金额。

✗ 不要惊慌。如果不确定，您可致电给家人或朋友，或拨打反诈骗热线1800–722–6688 寻求协助。

使用二维码并不危险，但网络罪犯可能会利用二维码将您引诱到钓鱼网站或启动包含恶意软件的下载。

ARE YOU CYBER SAFE?

Choose the right cyber tip to help you exit the maze.


START
Check that a link is legitimate
Download apps from third-party sources
Download any free app
Download apps from official sources
Postpone software or apps updates
Use passphrases with uppercase and lowercase letters, numbers or symbols
Use birth date as password
Read app reviews
Don't use 2FA
Enable 2FA
Update software and apps promptly
Don't use ScamShield or Anti-virus apps
Immediately click on a link
Add ScamShield and/or Anti-virus apps
END

Better cyber safe than sorry

Well done! You're Cyber Safe!