IFT

Feeding the minds that feed the world

Protecting IFT Sections from Cyber Threats

Cybersecurity is critical for protecting IFT Section's data, finances, and member information. This guide helps identify threats and implement best practices to maintain security.

Phishing Emails & Scams:

Be cautious of emails requesting urgent actions, like transferring funds or updating login credentials. Always verify unexpected requests by directly contacting the sender through a known phone number.

Types

5 COMMON TYPES OF PHISHING

EMAIL PHISHING
Scammers create emails that impersonate legitimate companies and attempt to steal your information.

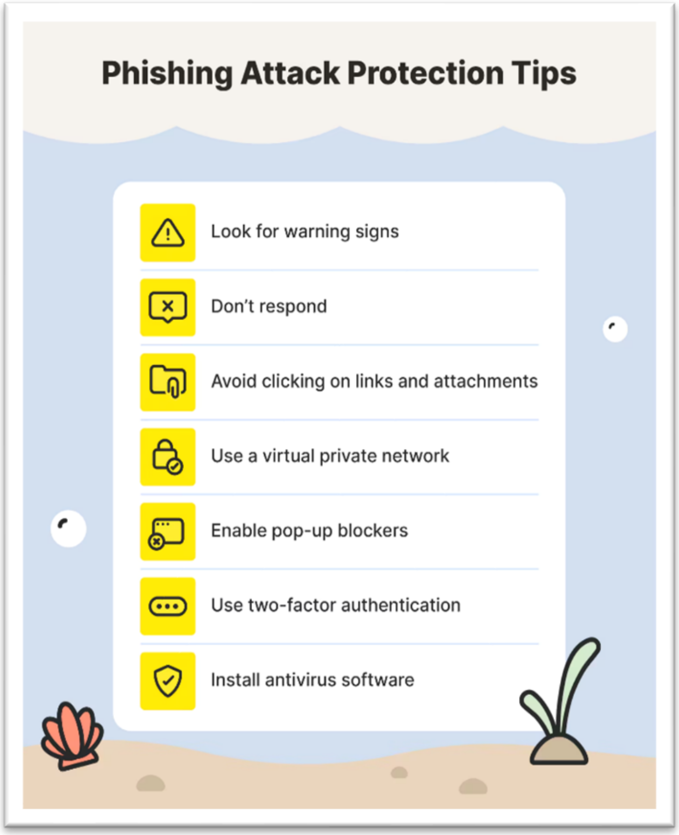
SPEAR PHISHING
Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.

CLONE PHISHING
Scammers replicate an email you have received, but include a dangerous attachment or link.

WHALING
Scammers target high-ranking executives to gain access to sensitive data or money.

POP-UP PHISHING
Fraudulent pop-ups trick users into installing malware.

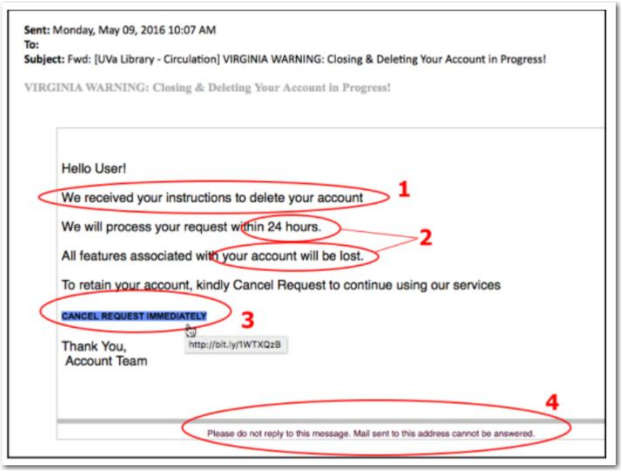
Tips



Phishing Attack Protection Tips

- Look for warning signs
- Don't respond
- Avoid clicking on links and attachments
- Use a virtual private network
- Enable pop-up blockers
- Use two-factor authentication
- Install antivirus software

Phishing Message Example



Sent: Monday, May 09, 2016 10:07 AM
To:
Subject: Fwd: [UVa Library - Circulation] VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

Hello User!

We received your instructions to delete your account

We will process your request within 24 hours.

All features associated with your account will be lost.

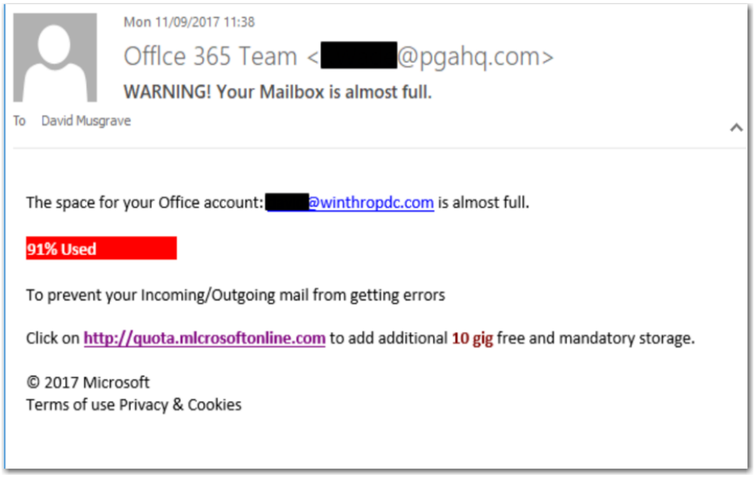
To retain your account, kindly Cancel Request to continue using our services

CANCEL REQUEST IMMEDIATELY

http://bit.ly/1WTXQzB

Thank You,
Account Team

Please do not reply to this message. Mail sent to this address cannot be answered.



Mon 11/09/2017 11:38

Office 365 Team <[redacted]@pgahq.com>

WARNING! Your Mailbox is almost full.

To David Musgrave

The space for your Office account:[redacted]@winthropdc.com is almost full.

91% Used

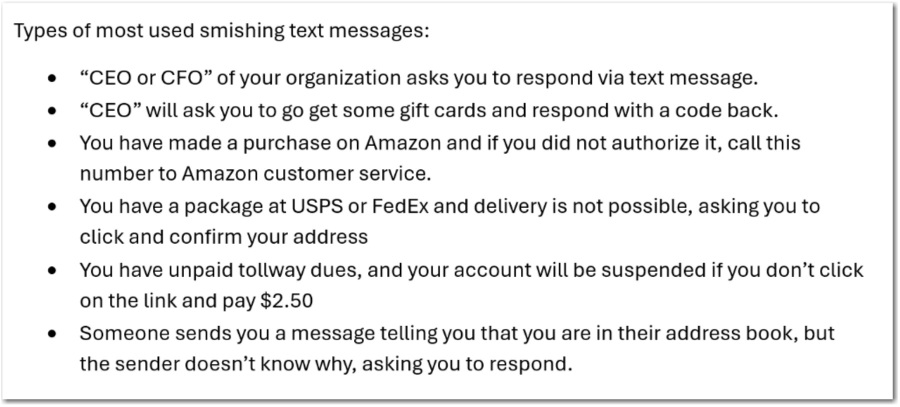
To prevent your Incoming/Outgoing mail from getting errors

Click on http://quota.mlcrosoftonline.com to add additional 10 gig free and mandatory storage.

© 2017 Microsoft
Terms of use Privacy & Cookies

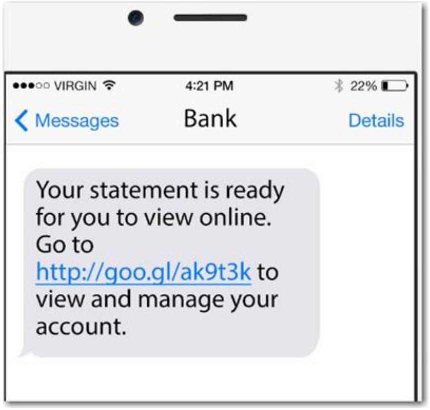
Smishing Messages

Smishing messages, similar to phishing but sent via text to your smartphone, can impersonate trusted entities to lure individuals into disclosing confidential details or to provide credit card information.



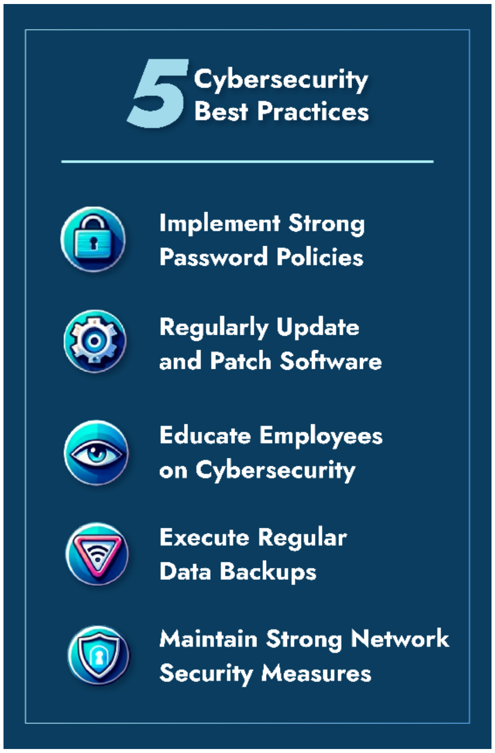
Types of most used smishing text messages:

- "CEO or CFO" of your organization asks you to respond via text message.
- "CEO" will ask you to go get some gift cards and respond with a code back.
- You have made a purchase on Amazon and if you did not authorize it, call this number to Amazon customer service.
- You have a package at USPS or FedEx and delivery is not possible, asking you to click and confirm your address
- You have unpaid tollway dues, and your account will be suspended if you don't click on the link and pay $2.50
- Someone sends you a message telling you that you are in their address book, but the sender doesn't know why, asking you to respond.



Your statement is ready for you to view online. Go to http://goo.gl/ak9t3k to view and manage your account.

Best Practices:



5 Cybersecurity Best Practices

- Implement Strong Password Policies
- Regularly Update and Patch Software
- Educate Employees on Cybersecurity
- Execute Regular Data Backups
- Maintain Strong Network Security Measures

What to Do If You Suspect a Cybersecurity Issue:

- Stop and verify – Do not respond or act immediately.
- Alert your leadership team – Immediately inform key Section leaders about suspicious activity.
- Report the incident – Notify IFT Headquarters at sections@ift.org
- Secure accounts – Change passwords and review access permissions.

For additional cybersecurity resources, visit JP Morgan Cybersecurity Awareness