What is the Value of a Hacked Email?

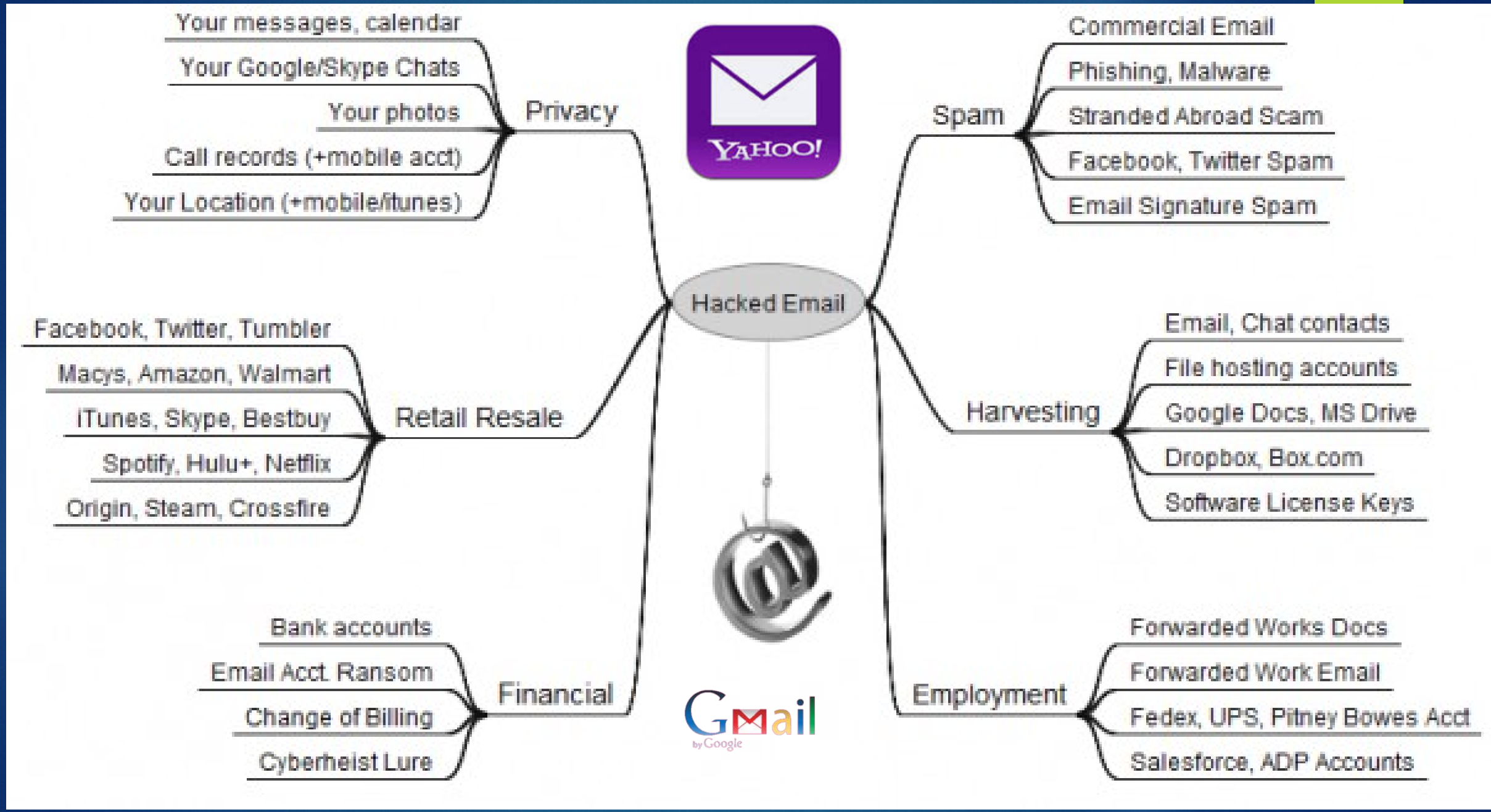
MOST PEOPLE DO NOT FULLY REALIZE HOW MUCH THEY HAVE INVESTED IN THEIR EMAIL ACCOUNTS UNTIL THOSE ACCOUNTS ARE IN THE HANDS OF CYBER THIEVES.

Mississippi Federal Credit Union

This presentation’s purpose is to make you aware of the street value of a hacked email account, as well as people, personal data, and resources that are put at risk when users are negligent in properly safeguarding their inboxes. Examples of Phishing Schemes and Security recommendations are included as well.

- Phishing is the fraudulent practice of sending emails pretending to be from reputable companies in order to coerce individuals to reveal personal information, such as credit card numbers, account numbers and passwords. All of phishing emails have a link provided that if invoked will either direct you to a site and infect your pc with malware (such as ransomware) or direct you to an website asking for personal information.
- Today when you sign up with any service online, it will require you to supply an email address. In nearly all cases, the person who is in control of that email address can reset the password of any associated services or accounts merely by requesting a password reset via email.

The chart below illustrates the ways that bad guys can gain monetarily by hacked computers.


Hacked Email
Privacy
Your messages, calendar
Your Google/Skype Chats
Your photos
Call records (+mobile acct)
Your Location (+mobile/itunes)
Spam
Commercial Email
Phishing, Malware
Stranded Abroad Scam
Facebook, Twitter Spam
Email Signature Spam
Retail Resale
Facebook, Twitter, Tumbler
Macys, Amazon, Walmart
iTunes, Skype, Bestbuy
Spotify, Hulu+, Netflix
Origin, Steam, Crossfire
Harvesting
Email, Chat contacts
File hosting accounts
Google Docs, MS Drive
Dropbox, Box.com
Software License Keys
Financial
Bank accounts
Email Acct Ransom
Change of Billing
Cyberheist Lure
Employment
Forwarded Works Docs
Forwarded Work Email
Fedex, UPS, Pitney Bowes Acct
Salesforce, ADP Accounts

Your email account may be worth far more than you ever imagined!

How much are hacked accounts worth? There is not a central exchange for hacked accounts in the cybercrime underground, but recent prices listed below are posted by several bad guys:

iTunes accounts - $8 each.

Fedex.com, **Continental.com** &**United.com** accounts -$6 each.

Groupon.com accounts - $5 each.

Godaddy.com, host provider, wireless providers **Att.com**, **Sprint.com**, **Verizon.com**, and **Tmobile.com** accounts - $4 each.

Facebook & **Twitter** active accounts - $2.50 each.

Dell.com, **Overstock.com**, **Walmart.com**, **Bestbuy.com**, **Target.com, etc.** Reduced rate of $1 - $3 (Discounted Crime Shops)

Stolen W-2 forms $2 - $20 each.

Think Information Inbox

Do you pay bills online? Do you have an iphone account, have you purchased software that has a license key somewhere in your messages?

Do you use online or cloud based file storage services like **Dropbox**, **Google Drive** or **Microsoft Skydrive** to back up your pictures, files and music? Is the key stored in your inbox?

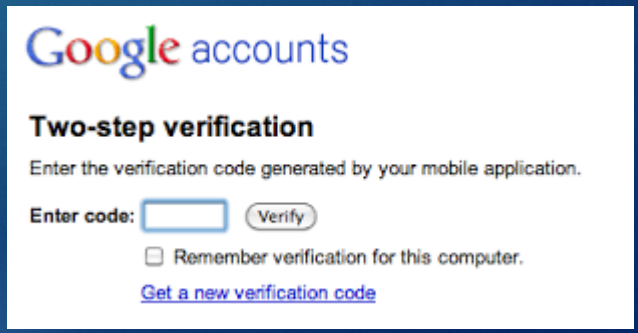
Hacked email accounts are not only used to blast junk messages; they are harvested for the email addresses of your contacts, who can then be inundated with malware spam and phishing attacks.

Multi Step Authentication:

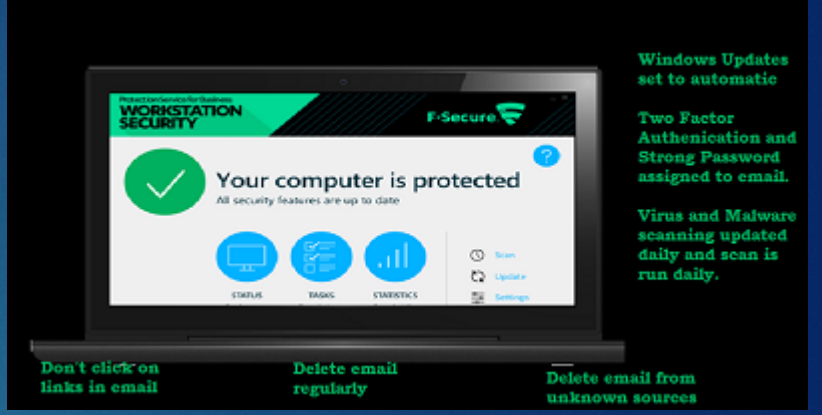
If your inbox was held for ransom, would you pay to get it back? If your Webmail account got hacked and was used as the backup account to receive password reset emails for another Webmail account, guess what? Attackers could then seize both accounts.

If you have corresponded with your financial institution via email, chances are decent that your account will eventually be used in an impersonation attempt to siphon funds from your bank account.

Until recently, some of the Web's largest providers of online services offered little security beyond a username and password. Today the larger providers have moved to enabling multi-factor authentication to help users avoid account compromises. Gmail.com, Hotmail/Live.com, and Yahoo.com all offer multi-step authentication that users can and should use to further secure their accounts. Dropbox, Facebook and Twitter also offer additional account security options.



Additional Security can be defeated if the bad guys gain control over your machine through malicious software.



- Keep patches current on your windows workstation.
- Be cautious of JavaScript, which has few options to control scripting in Internet Explorer, but Firefox and Chrome have options to control the running of JavaScript.
- Keep virus software and malware software updated, but remember that the software can only scan for ‘known’ viruses and malware. Surf with the realization that there are new malware programs being released every day.
- Assign passwords that are strong, minimum of 8 characters, Upper case and lower case, special characters and numbers. Consider using pass phrases and use two step authentication when offered.
- Make sure that your wireless router is secure. Always change the manufacturers default password. If you are unsure as to your security, contact a 3rd party vendor to secure it.
- Use caution when downloading software or files from the web.
- Attachments and links in emails from unknown sources should be deleted.

Phishing Emails and Variations:

Business Email Compromise (BEC Scam) is a form of phishing that is rampant today and targets specific people within a business by impersonating an executive or other person that may do business with the organization. As the name suggests, it's a scam using email messages in the hope that the recipient will not check for authenticity before performing a requested task. According to the FBI, costs to businesses because of BEC have exceeded $3 billion and that number continues to rise. The FBI has received complaints about this type of fraud from victims in every state in the U.S. and in at least 79 countries. It affects organizations of all sizes and does not discriminate based on industry or sector.

The FBI reports that there are two variations of the BEC scam, known as **CEO fraud** and **W-2 Phishing.** Both scams start with an email account compromise for high-level business executives (CEO,CFO, etc). Posing as the executive, the fraudster sends a request for a wire transfer and a request for employees W-2 forms from the compromised account to a second employee within the company who is normally responsible for processing these requests. The requests for both are well-worded, specific and do not raise suspicions.

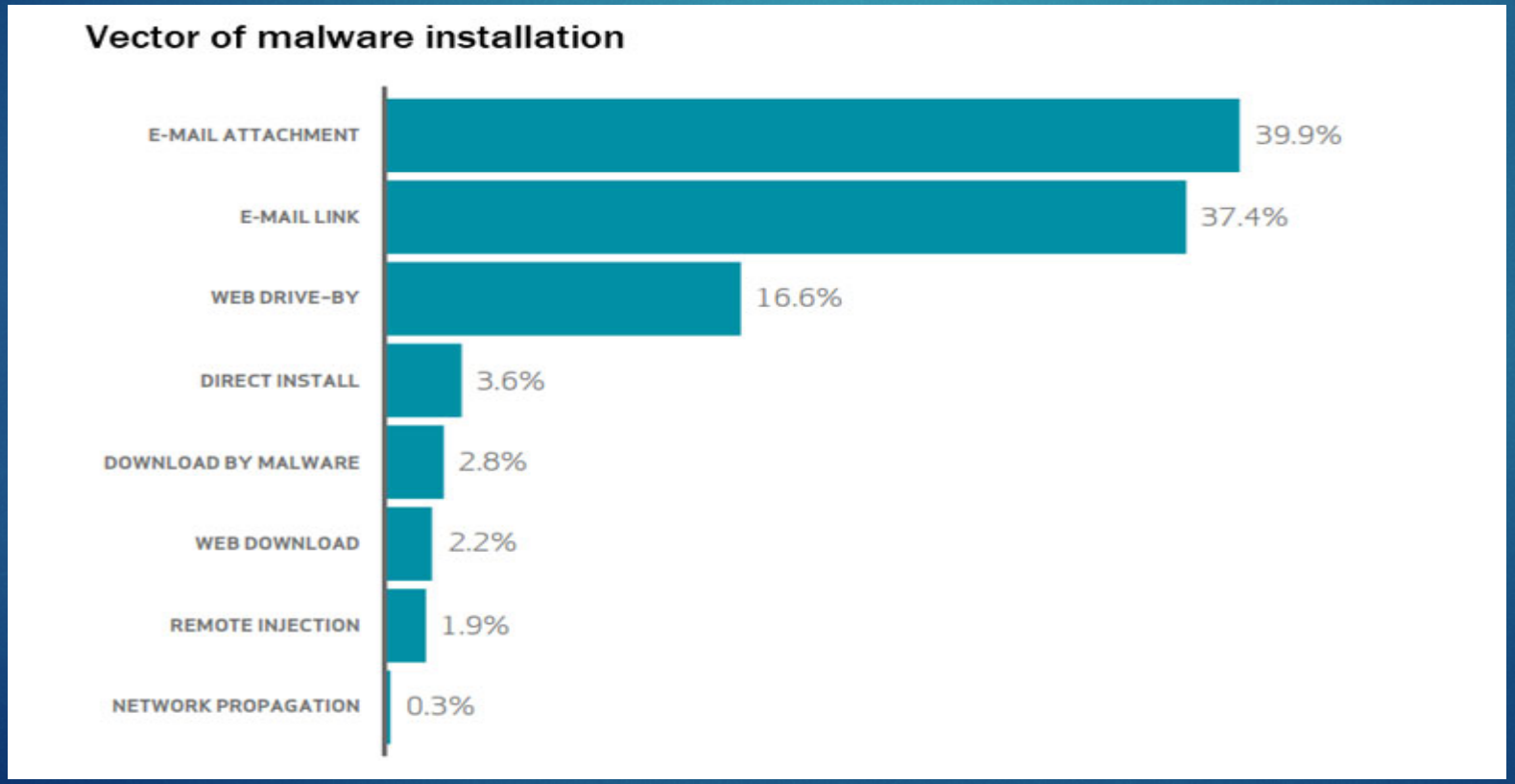
Additionally, the IRS has sent out an urgent alert that warns companies of the W-2 Phishing scam and that it is being combined with the CEO Fraud Scam. They note that the scams have begun earlier in 2017. The W-2 scam surfaced in February of 2016.

The Internet Crime Center notes that the fraudsters perpetrating these scams do their homework before targeting a business and its employees, monitoring and studying their victims prior to initiating the fraud using social media and other methods to gather information regarding travel, etc. An ICC alert warns that fraudulent e-mails received have coincided with business travel dates for executives whose e-mails were **spoofed.** Victims may also first receive 'phishing' e-mails requesting additional details of the business or individual being targeted (name, travel dates, etc.). **Spoofed email** is the creation of **email** messages with a forged sender address.

The advisory urges businesses to adopt two-step or two-factor authentication for email, where available, and/or to establish other communication channels — such as telephone calls — to verify significant transactions. Businesses are also advised to exercise restraint when publishing information about employee activities on their Web sites or through social media.

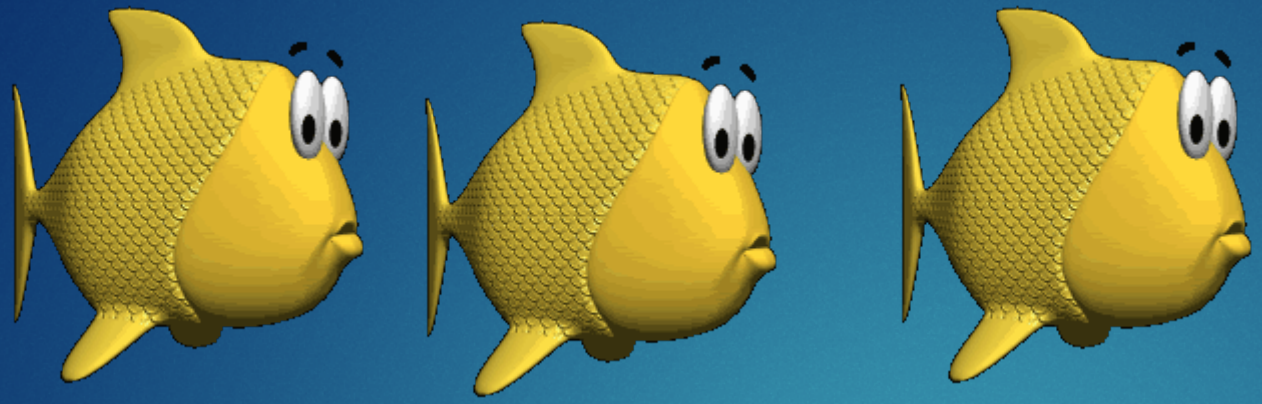
Verizon Studies and Reports on Phishing Emails

- Verizon reported that 30% of the recipients targeted for phishing emails actually open the messages.
- They also found that 12% of them actually click on malicious links or attachments.
- No matter how many technical security tools are in place, they will not keep 100% of phishing email out of anyone's in box.
- Awareness and education will always be necessary.



ID Phishing Email:

- **Did You Expect the Link**: Always be wary of links or attachments that arrive in email messages that are *not expected*.
- **Check the Link Destination**: If you want to do an extra check of a link, hover over it with your mouse to see where it goes.
- **Grammar and Spelling Mistakes**: Although these are found less often now, if there are spelling or grammatical mistakes, it should be considered suspicious.
- **Urgent or Threatening Language**: If the email uses language that makes it sound threatening or urgent, take some extra time to evaluate it.
- **Verify Financial or Sensitive Information Requests**: Take a moment to verify any request for a transfer of money or to send sensitive information via email.
- **No One Needs Your Credentials**: Never give out credentials for financial accounts to anyone. No one that truly has access should need yours.
- **Be aware of shared information on social media and networking sites**: When on any site, please be very cautious of what personal information you provide.



Don’t take the hook with false bait and get caught!

Pay close attention to emails received and do not assume that all email is safe.