Cybersecurity tips

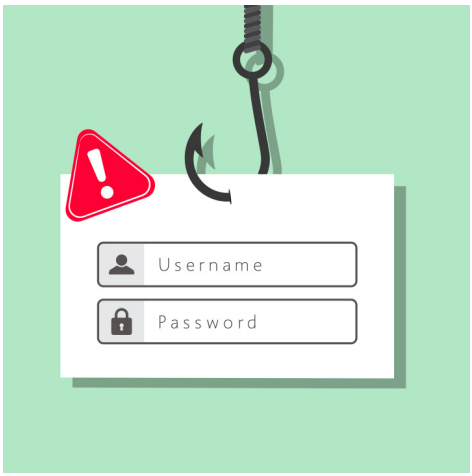
Emails and fraudulent websites are increasingly attempting to lure people to click malicious links.

Websites or email attachments may request a username and password to access content, but only serve to capture your credentials. Similar requests are also being received by text and SMS messages.

Once you click on the link and enter your credentials, there is the potential to compromise the entire Black& McDonald network, as well as any personal information stored locally on the computer.

A compromised computer or network can cost countless hours to restore and can be devastating financially should data be encrypted or stolen.

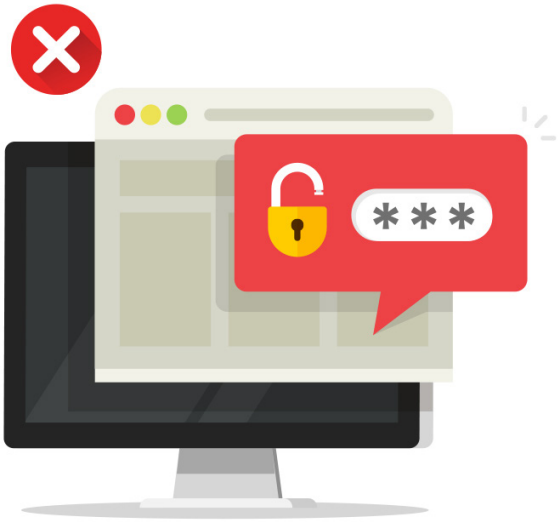
Do not open an email attachment or click on a link if you do not know the sender or are unsure you are the intended recipient.



If you click on a suspicious link or document, or enter your password on any document or site, notify the IT Service Desk immediately. **As call times may be longer during this period, change your password immediately!**

Don’t be fooled if you receive an email that is addressed to you. Even though the sender knows your name, it could still be an attempt to trick you.

Inspect all email thoroughly before clicking on a link or opening an attachment. Watch for poor grammar or messages that give a sense of urgency. If something feels off, trust your instincts! Hover over the email address or link to reveal its source.



Never type your credentials into a link or message received from an email, text or SMS.

Be vigilant in protecting sensitive information. If you are unsure or have questions about any content you have received, contact the IT Service Desk immediately.

The IT Service Desk is available Monday to Friday, 7am to 6pm EST

Phone: 1 (866) 626-6022