# Security Awareness /Trends

December ‘17

SECURITY TIPS FOR THE HOLIDAY SEASON

## Security Tips for the Holiday Season

### ‘Tis the Season for Cyber Security

The holiday season finds many of us overwhelmed but don’t let this busy time catch you off guard. Unfortunately, this season can leave us all more vulnerable at a time when the risk of cyber threats are known to be on the rise. Cyber Grinches will typically ramp up their malicious activities during the holiday season in the form of holiday-specific spam, spear phishing or compromised websites. However, here is a reminder of what to be on the lookout for.

### Watch your Inbox

Phishing is still the number one way in which the bad guys attempt to gain access into your computer or our college network. JCCC recently was targeted by a phishing attack. Phishing is a type of cyber-attack that attempts to obtain sensitive information such as usernames, passwords, or financial information, by disguising itself as a trustworthy entity in an email message. The message that was sent to JCCC staff with the subject “Your Email Has Exceeded Quota Limit” was such an attack. Inside the email was a hyperlink to “sign-in” to your email account. This link if you were to hover over it without clicking on it would have taken the victim to a web site that was designed to look like the Microsoft 365 login portal but was in reality a web site controlled by the attacker designed to capture usernames and passwords. Here is a short list of things to look for in an email to help you spot a phishing attack.

1. **Verify the senders email address.**
2. **Pay close attention to embedded hyperlinks and where they point.**
3. **Don’t give out personal information.**
4. **Beware of urgent or threatening language.**
5. **Don’t open unexpected attachments.**

The phishing attack that impacted JCCC leveraged a compromised internal account to bypass protections in place to filter forged sender emails. Aligning this message with the tips above we see the urgent tone in the subject line. The message also had an embedded link that was designed to draw the user to a forged malicious site in France.

When the phishing attack occurred Information Services responded by removing the message from users’ inboxes. As a result many staff may never have seen the message in their email. A block was also placed on the website that was hosting the malicious webpage so that it was not accessible from on campus. We notified staff of the threat and its impact and worked with the Technical Support Center (TSC) to assist any staff that may have been impacted. We’ll be updating our annual security awareness training to include focused information around identifying these attack types.

### Goodwill to All

We all share the responsibility of providing a secure computing environment and protecting our digital assets. If you receive a suspicious email with attachments or attempting you to provide sensitive information, alert IT security at infosec@jccc.edu.

Federal Bureau of Investigation, Holiday Shopping Tips, https://www.ic3.gov/media/2012/121120.aspx (accessed Dec. 2017)