

SECURITY AWARENESS

STEVEN ALEXANDER

DIRECTOR OF IT SECURITY, KCCD

PASSWORDS

TOP 3 TIPS



#1 NEVER SHARE OR GIVE AWAY YOUR PASSWORD

- Don't share it
- Don't put it in an email
- Don't ever click on a link to “verify” your password or account*
- Don't give it to the IT department

#2 PASSWORDS AND POST-ITS DON'T MIX

- It's okay to write down your passwords, just keep them in a safe place like your wallet or a locked cabinet/drawer
- Do NOT put them on sticky notes on your monitor or under your keyboard
- The best solution is to use password management software like KeePass or 1Password
 - Unfortunately we don't have an officially supported option

#3 PICK A STRONG PASSWORD

- A strong password is generally 15 characters or longer
 - Double passwords like “PasswordPassword” don’t count.
 - Obvious patterns are still weak: QWERTY1234567890
 - Try a passphrase:
 - “Mycatwearspurplesocks!” ←22 characters, nonsensical, hard to guess
 - Don’t pick quotes or song lyrics:
 - “Maytheforcebewithyou” ←Long, but easy to guess

POPULAR SCAMS



GIFT CARD SCAMS

- Scammers are emailing employees pretending to be their managers.
- “Are you at your desk”
 - “I need a favor.”
 - “I need you to buy some iTunes gift cards...”
- Make sure your employees know you will **never** make a request like this.

I KNOW WHAT YOU DID

- I hacked your computer and your webcam
- I know what sites you went to
- I saw you
- Pay me not to embarrass you

VERIFY YOUR ACCOUNT

- “We’re updating our email system...”
- “Your mailbox is full...”
- “There was a suspicious login...”

PLEASE CLICK HERE TO VERIFY YOUR ACCOUNT 😊


LINKS



SAFE LINKS

Reply Reply All Forward IM

Fri 3/1/2019 11:46 AM

 Steven Alexander

9 to 5 mac - test email

To Steven Alexander

<https://na01.safelinks.protection.outlook.com/?url=https://9to5mac.com/2019/02/28/spectre-long-exposure-camera-app/&data=02|01|steven.alexander@kccd.edu|eb01cc53d0994544531e08d69e7e9880|52a30add642a46f8a4e2c61db3eb8742|0|0|636870663892216329&data=be6ozlgpwevuch5uozbm/a8bobcc4gel+ze2x04w+04=&reserved=0>
Click or tap to follow link.

<https://9to5mac.com/2019/02/28/spectre-long-exposure-camera-app/>

Steven Alexander
Director of IT Security
Kern Community College District
(661) 336-5111



This link is being scanned.

We're scanning this link to see if it is malicious.

`www.unsafe_url/login.php`

We're scanning this link to see if it's malicious. The scan should be completed soon, so try opening the link in a few minutes.

X Close this page

[Continue anyway \(not recommended\)](#)

Powered by [Office 365 Advanced Threat Protection](#)

DON'T CLICK LINKS IN EMAIL

- If you can avoid it, don't click links in Email
- Bookmark sites such as Gmail, Facebook, Amazon, Wells Fargo
- Use your bookmarks instead of email links
- Type in the addresses manually if you can
- Google if you must but bookmark it for future reference

ATTACHMENTS



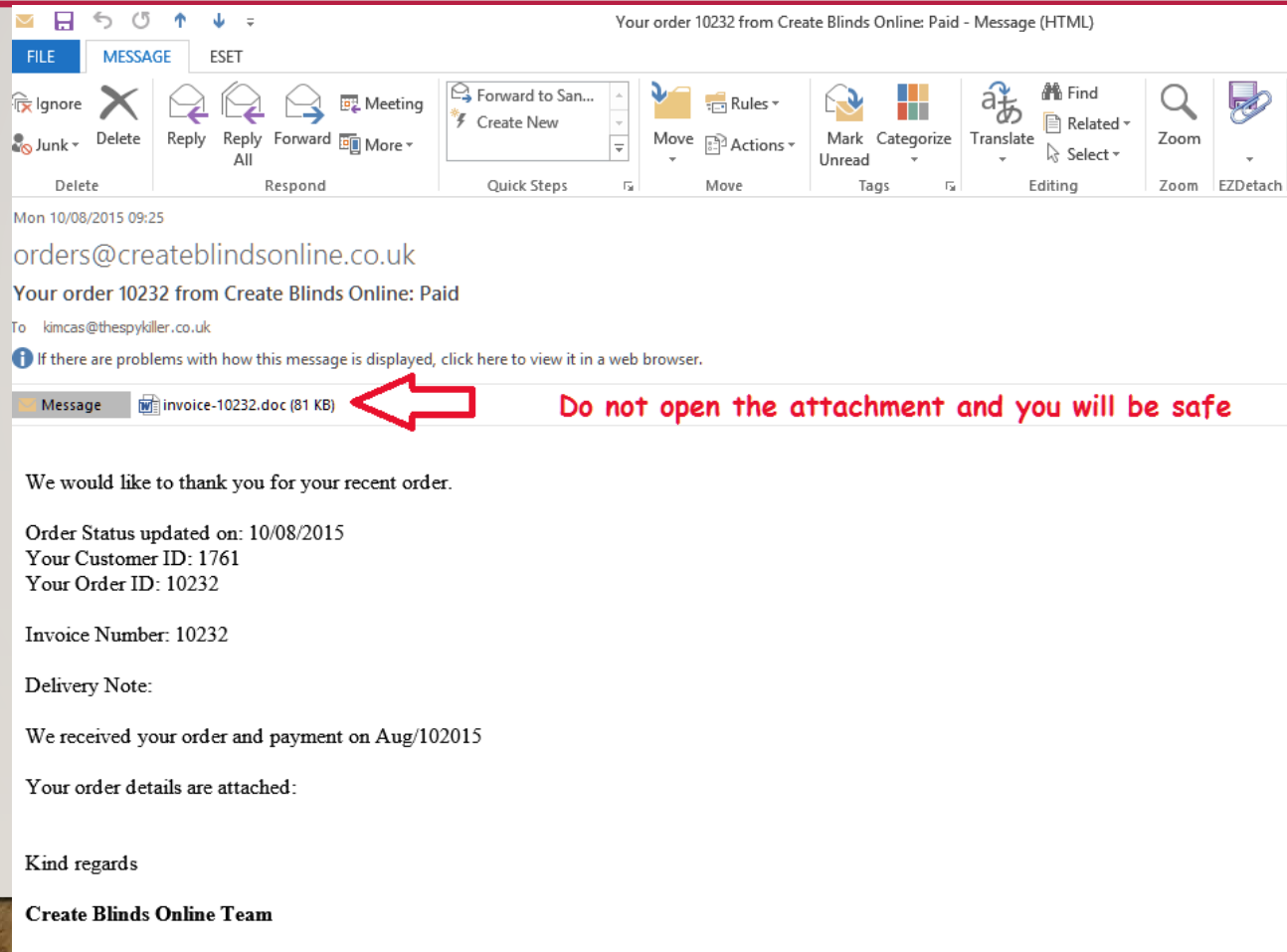
UNSOLICITED ATTACHMENTS

- An unsolicited attachment from an unknown person should be treated with suspicion.
- If you think that it might be legitimate but are not 100% sure, contact IT for assistance.
 - Report-spam@kccd.edu
- The safest option is to delete it.

UNEXPECTED ATTACHMENT FROM A KNOWN SENDER

- If you receive an unexpected attachment from someone you know, call them.
- Be very cautious if the message seems atypical for this sender:
 - Different contact information
 - Bad grammar

WHEN IN DOUBT, DON'T OPEN THE ATTACHMENT






Mon 10/08/2015 09:25

orders@createblindsonline.co.uk

Your order 10232 from Create Blinds Online: Paid

To kimcas@thespykiller.co.uk

 If there are problems with how this message is displayed, click here to view it in a web browser.

Message  invoice-10232.doc (81 KB)  **Do not open the attachment and you will be safe**

We would like to thank you for your recent order.

Order Status updated on: 10/08/2015
Your Customer ID: 1761
Your Order ID: 10232

Invoice Number: 10232

Delivery Note:

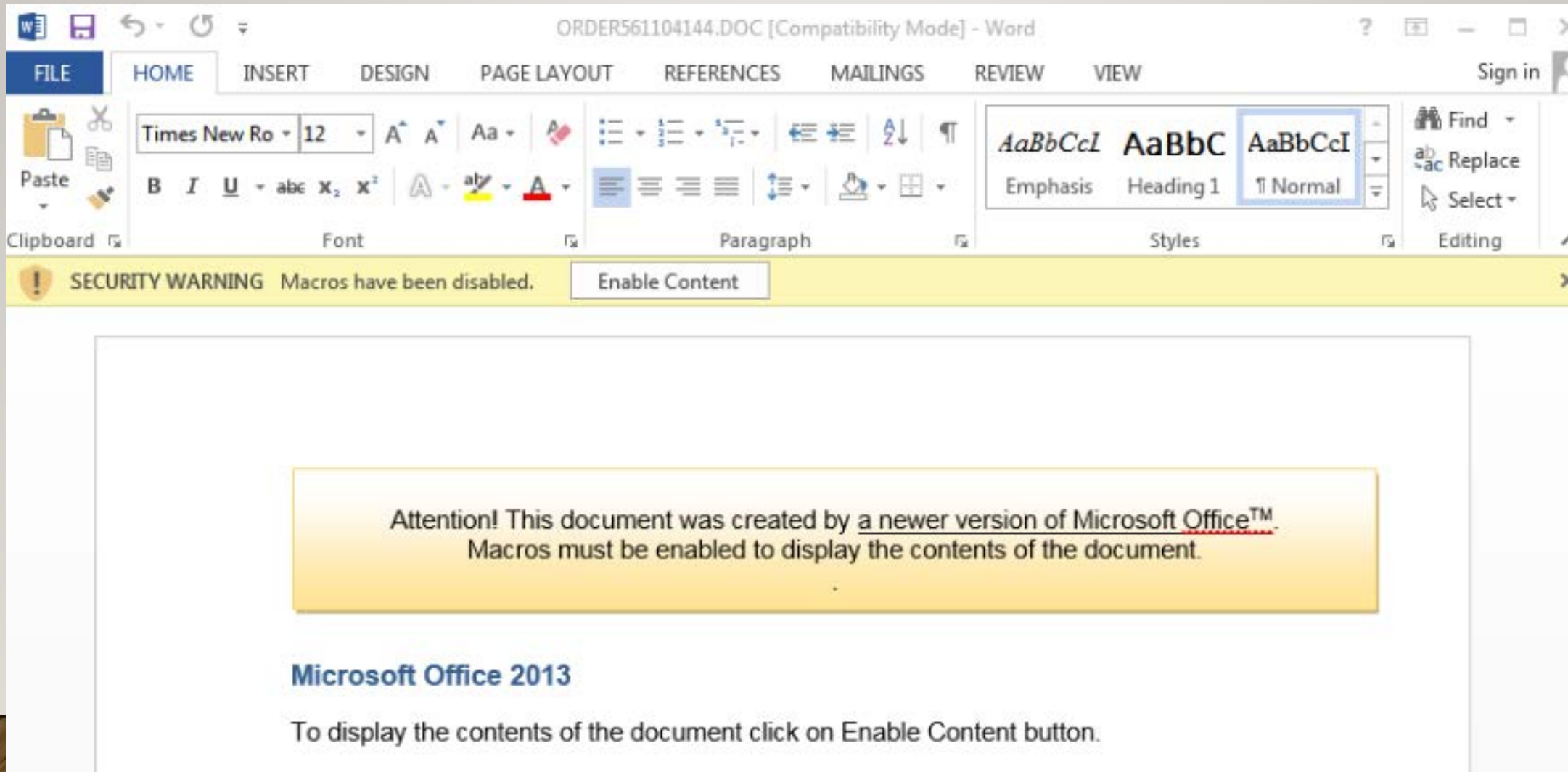
We received your order and payment on Aug/102015

Your order details are attached:

Kind regards

Create Blinds Online Team

ENABLE CONTENT IS A WARNING SIGN



The image shows a screenshot of the Microsoft Word interface. The title bar reads "ORDER561104144.DOC [Compatibility Mode] - Word". The ribbon is set to the "HOME" tab, with sub-tabs for "FILE", "HOME", "INSERT", "DESIGN", "PAGE LAYOUT", "REFERENCES", "MAILINGS", "REVIEW", and "VIEW". The ribbon includes sections for "Clipboard", "Font", "Paragraph", "Styles", and "Editing". A yellow warning banner at the top of the document area reads: "SECURITY WARNING Macros have been disabled." with an "Enable Content" button. Below the banner, a large yellow box contains the text: "Attention! This document was created by a newer version of Microsoft Office™. Macros must be enabled to display the contents of the document." Below this box, the text "Microsoft Office 2013" is displayed in blue, followed by the instruction: "To display the contents of the document click on Enable Content button."

ORDER561104144.DOC [Compatibility Mode] - Word

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW

Clipboard Font Paragraph Styles Editing

SECURITY WARNING Macros have been disabled. Enable Content

Attention! This document was created by a newer version of Microsoft Office™. Macros must be enabled to display the contents of the document.

Microsoft Office 2013

To display the contents of the document click on Enable Content button.

ENABLE CONTENT, SOMETIMES?

- If you are used to clicking Enable Content or Enable Macros for certain documents, you can keep doing so. But, you need to know that the document is safe, first.
 - If you're not sure, ask!
- If the document warns you that you must click Enable because you're using an "old version" or that you should click if you "can't see the numbers", it's a trick.

REPORT SUSPICIOUS EMAILS



WHAT TO DO IF YOU RECEIVE A PHISHING EMAIL

- 1) Forward the email to report-spam@kccd.edu
- 2) Delete the email

You can forward emails to us even if you're not sure and just want us to check it out.

QUESTIONS?

