The IT Insider

1

September 2018

6 SCARY EMAILS YOU SHOULD NEVER OPEN

If you aren't extremely vigilant about your email inbox,

you could be in for a nasty malware surprise.

These are the emails you should never, ever open.

If the email is from your bank, give them a call and verify the message is legitimate (it's probably not - banks will call you if they discover unusual account activity).

The internet can be scary, but emails are the scariest. Email is the #1 way hackers are able to get into your small business' network. Unsurprisingly, people are much easier to trick than security systems like firewalls and anti-virus. If you aren't extremely vigilant about your email inbox, you could be in for a nasty malware surprise.

Here are the 6 scariest emails you should never, ever open.

Confirm Your Account / Unusual Login Activity

You use the Internet to log into multiple important websites every day. Likely, you do your banking online. You may pay your bills online. You shop online. And of course, we all have social media accounts. BUT, you should never open emails suggesting a password change or an account confirmation. Instead, delete the email, and then log into the appropriate website. You can change your password directly in Facebook instead of clicking on a link in an email that may infect your computer. If the email is from your bank, give them a call and verify the message is legitimate (it's probably not - banks will call you if they discover unusual account activity).

You Missed a Delivery

UPS and Amazon are both big favorites of hackers who want to target small businesses. If you receive an email from UPS, USPS, Amazon, etc claiming that you missed a delivery - don't open it. Especially don't click on anything. Log into your various mailing accounts and review your tracking activity. Are you even expecting a delivery? It's also very easy to pick up the phone and give the company a call and verify that a package was unable to be delivered.

Your Account has been Locked

It probably hasn't been. If you get an email like this one, be very very careful not to click any button to unlock your account (whether it's Facebook or LinkedIn or Chase). Instead, use the same method as I mentioned in the first of the scary emails: try logging into the account directly from a new window. It's probably not locked at all. In the event that it is, give the company a call and ask about the next steps you can take.

Unexpected Refunds or Payments

Don't fall for this one, either! Think about it - how likely is it that you are owed a refund for something you hadn't even thought about? Why are you being paid for something you're not sure you did? Instead, call up the sender of these sorts of emails to verify their legitimacy. Do not open any attachments claiming to be payments or refund vouchers.

Ask yourself - why am I getting this email? Does this email make sense?

Delete the email. If you're actually owed that money, the sender won't mind sending it a second time.

Resume Attached / Invioce Attached

So, you've received a resume in your inbox. Ask yourself - why am I getting this email? Is my company hiring? Am I the correct person to receive a resume? Is there any email content that indicates who the resume belongs to? Best case - you delete an email from an honest person trying to get a job, and in that case, you can call them to verify the email. Worst case - it's a ransomware virus and you lose everything.

CEO Fraud

We've saved the best (worst?) for last. Emails from your CEO that aren't really from your CEO. This is called 'spoofing', and it's becoming more and more common. If the email seems strange, don't open it. If there's a link inside the email, don't click it. Does the email make sense or is it simply asking you to fill out an unidentified form? If you're not sure, contact your boss about it. He'll likely be relieved to find out his email is being spoofed and you didn't fall for it. Urge him to contact your IT support about the issue, though, since once an email gets spoofed, it can be used over and over again by the hacker until that avenue is closed.

How well do you think you'll remember these specific rules in a couple weeks when you're going through your inbox uncaffeinated? What about your employees? The good news is - people can be trained! A little knowledge can go a long way. If you'd like to sign up for security awareness training, let us know. It could save you thousands.

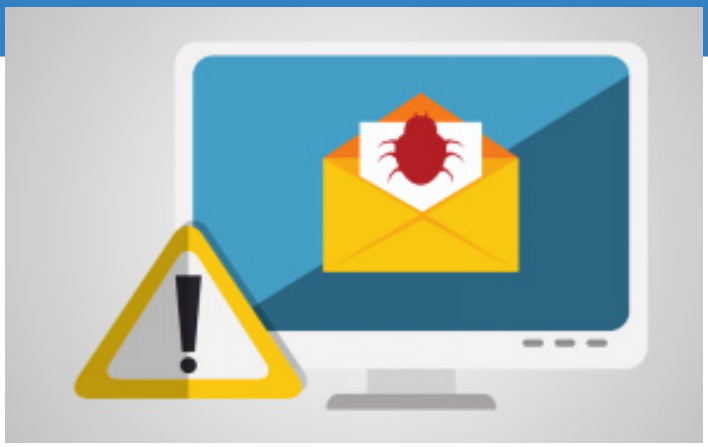
The delete button is your friend.

Congratulations Jordan!

Jordan joined our team in late August 2017, and has officially been a part of the Preferred IT family for one year.

He's a particular favorite of Office Dog Sully, who can frequently be found napping at Jordan's feet.

Here's to many more years to come! Thanks Jordan!



USE SOCIAL MEDIA LIKE A PRO

If you Google a business and nothing but the address and a strangely angled photo of their front door appear in the results, how can you be sure it's a legitimate business? Perhaps it closed down permanently? Who knows? Businesses need an online presence in order to even qualify as a "real business" these days. By communicating with buyers, customers, and industry peers, you are telling the world that you're here, you care, and you know what you're talking about. Most of all, you want to use social media to stay "top of mind" and increase sales. Even if a buyer only knows you because you answered their question on Twitter, they're still more likely to buy from you versus your competition.

Not all social platforms are created equal, though. So, here are some tips for using the most popular social platforms to your advantage.

Facebook works for every industry and is where most customers will communicate with you. It requires the least amount of upkeep but keeps you relevant just by existing (kind of like your website). Facebook is great for sharing photos, videos, blog posts, and fun personal content that your customers would be delighted to see.

Twitter has a much, much wider reach than Facebook. Your Facebook content reaches only your fans. Tweets, on the other hand, spread like wildfire through the use of hashtags. It's useful for marketing your services and handling customer service, but where it really shines is industry conversation.

LinkedIn is the third most important social platform (for most companies). It's perfect for professional networking and cultivating your industry leadership. Make sure to create a business page as well as improve your personal one. Keep things professional and fill out your profile as best you can.

Instagram is 100% visual and 100% mobile. A blurry photo of the company BBQ is not going to cut it here. It's essential that your photos are high quality and quickly digestible. Otherwise, people will scroll right past your content. Aesthetically pleasing graphics with quotes or announcements are perfect for Instagram.

All of these social platforms are not necessary for every (or any) business. You should choose the ones that make sense for your industry and your customers. Think about the kind of person or company you want to sell your product or service to - now do some research on where those people are spending their time online. By Googling "social media demographics", you will be well on your way to choosing which social platforms are best for your brand.

PREFERRED IT SECURITY SPOTLIGHT

Types of Cybercrime

Viruses are tiny computer programs that spread by infecting files and drives and then making copies of themselves. They work similarly to human viruses in that way. They are almost always spread through emails -- although certain downloads on your computer or your mobile device can contain viruses as well.To avoid accidentally installing a virus onto your computer, do not open any attachments in your email unless you are expecting it.

Spam emails are any unsolicited commercial emails. Of course, spam emails are usually legitimate and won't give you a virus of any kind. They're just annoying advertisements and bids for your business. However, they can also be used by cybercriminals to embed malicious links designed to install a virus on your computer. It's best to review your spam emails with a finger over the delete button.

Possibly the most difficult cybercrime to prevent is social engineering. **Social engineering** can be referred to as human hacking. While this is still a cybercrime because it utilizes the internet (and most often, email), social engineering is not designed to infiltrate a machine. Therefore, security measures like anti-virus and firewalls have zero effect. The cybercriminals use psychology to prey on their victims. It's important to be aware of your situation, and be overly cautious when divulging personal information. Cybercriminals are hoping that if they can scare you into believing your computer is broken (or your credit card has been stolen), you will play right into their trap.

Want To Know For Sure If Your Data Is Safe?

Thanks to our Done-For-You Disaster Recovery you can rest assured that your data is being backed up in a format that is not only secure, but also easily recovered when you need it.

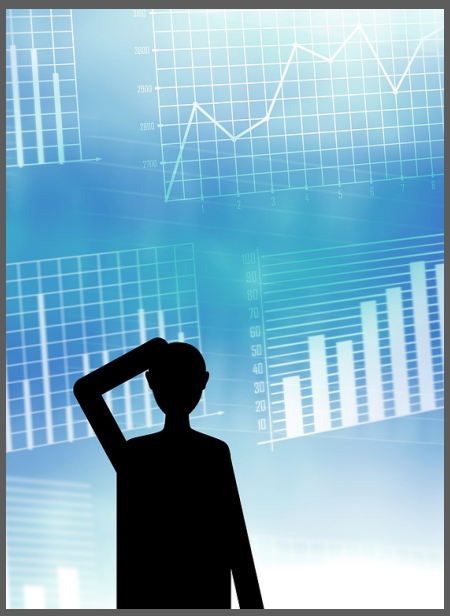
Your files are automatically backed up every hour locally and over the Internet.

Your data is safe from fire, floods, storms, viruses, hackers, hardware malfunctions, and human error! With image-based and file level backups, your data is immediately accessible even during a disaster.

Should a disaster occur, you can be back up and running the very same day…we **GUARANTEE** it.

Preferred IT Group will provide the hardware required, **absolutely free**.

Learn more at www.preferreditgroup.com/dfydr



OUR COMMUNITY

The weather is getting colder and that means getting your kids new coats, hats and gloves!

If your child has outgrown their gently used winter coat, please consider donating it to Preferred IT Group.

We are partnering with COATS FOR KIDS this year, as we do every year, to make sure every child in Fort Wayne has a warm coat this winter.

We will be collecting coats all the way through December, so drop by our office anytime!

preferred IT group

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.