VOLUME 3, ISSUE 2 APRIL, 2022

THE ITS QUARTERLY

A NEWSLETTER FROM INFORMATION TECHNOLOGY SOLUTIONS
GRAND JUNCTION, CO

celebrating ITS 15 Years! IN BUSINESS

IMPORTANT DATES:

Spring has Sprung

Please note the following dates we will be closed:

05/30/2022 - Memorial Day

As a reminder, we are open from 7a to 5p. If you need emergency support after hours, we have an on-call technician who can assist.*
You can also email us at: support@itsolutionsco.com and we will open a ticket the next business day to help with your issue.

*Additional fee may apply

DID YOU KNOW:

PHISHING & RANSOMWARE INCREASED SIGNIFICANTLY IN 2021

BY: AMELIA SANCHEZ

The 2021 threat landscape reinforced one key point: successful threat protection requires a people-centric defense. You must be a vital part of the security stack. The more informed and equipped you are from a cyber attack, the more resilient your company will be.

More than 1,100 phishing campaigns abused the Microsoft brand – using a Microsoft-themed lure or product to steal credentials or deliver malware. So as users of Microsoft O365, it's essential that you stay vigilant and look for the signs that clue you in that you have received a fake email.

There were more attacks throughout 2021 than 2020, confirming that attackers focused on taking advantage of the new office-home hybrid work environment that many companies have adopted since the beginning of the pandemic.

BUSINESS EMAIL COMPROMISE ATTACKS INCREASED ALMOST 20% IN 2021, FROM THE YEAR PRIOR.

Email is where you as a business person, employee, and owner need to concentrate the most to protect your company, your data, and your employees.

Continued on Page 2-3

Stay safe from Scammers: Tips for prevention!

Here are the best ways to prevent a phishing or ransomware attack:

Enable Multi-Factor Authentication. We can't say this enough. A password alone isn't enough to keep you safe online. MFA makes you 99% less likely to get hacked. This is a second layer of identification, confirming to wherever you're logging in to is in fact you. MFA is either a confirmation text message or email code, a code from an authentication app, a fingerprint or FaceID, or a token or FIDO key.

Update your software and activate automatic updates. Even the most reliable programs can have undiscovered vulnerabilities that hackers will take advantage of. Responsible manufacturers will release patches to address security flaws as soon as they are revealed.

Use strong passwords. Once again for those sitting in the back: ***USE STRONG PASSWORDS!***

The longer the password, the better. An ideal strong password will be 13 characters or longer and include letters, numbers, and characters. Do not keep the same password for every login.

Think before you click. If it looks phishy, and smells phishy, then it's probably a phish! Trust your instincts and don't click the odd link. See the next page for red flags.

Adding an email filter gives an additional layer of security. With this in place, you will not see the majority of spam sent to your inbox.

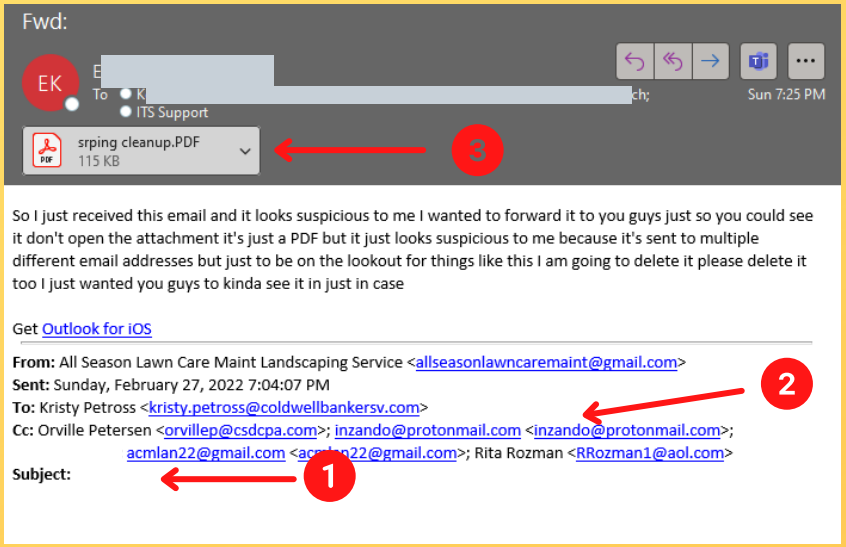
Back up your data. If the worst-case scenario occurs, and your data is hijacked by ransomware, having backed up your data takes the power away from the attacker. You won't need to pay a ransom to get it back, because you already have a copy of it.

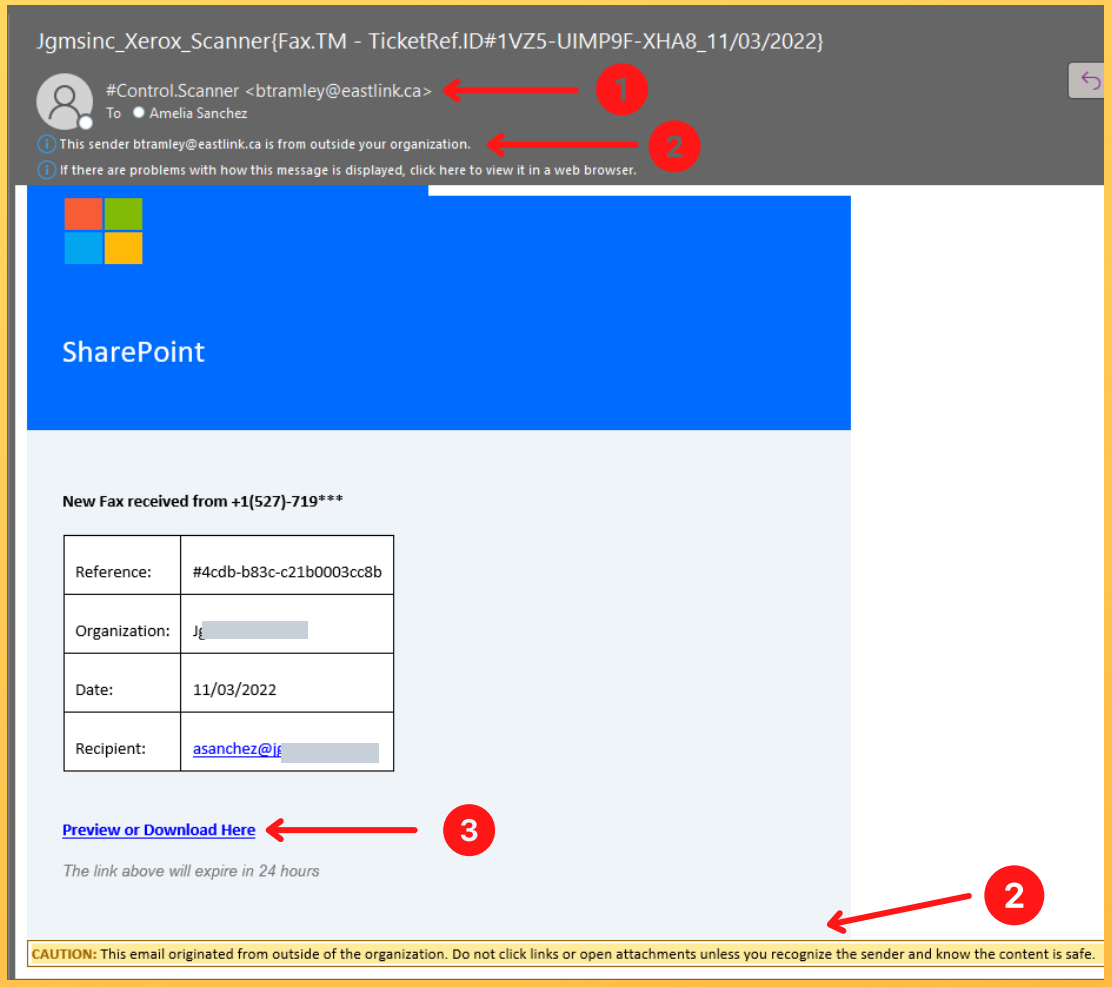
Phishing Emails: What to look for

The email to the right was forwarded to us by one of our clients.

Clues that this is a phishing email:

1. There is **no subject** written in the subject line.
2. The client was sent this email in **a group of people they don't recognize.**
3. Check the **spelling error** in the attached PDF. "srping" is not how you spell "spring."





Example of a phishing attempt on one of us:

1. **Don't trust the Display Name.** This does not match any part of the email address associated with it.
2. There are two notifications that state this email **originated from outside the organization.** While you may receive many emails from other orgs/clients/customers, this security measure was set in place to visually clue the user in that this may be a scam.
3. Hover over the link in the email. If the actual URL that appears does not match or you do not recognize it, **DON'T CLICK IT.**

THE MORAL OF THE STORY IS, YOU ARE YOUR BIGGEST DEFENSE AGAINST CYBER-ATTACKS.

The more security protocols you put in place, the better off you and your company will be. Keep in mind, though: **there is always the possibility of a scam getting to you.** The best way to prevent yourself from falling for it, is to be aware of the signs. If you are interested in training your employees on how to be more aware, reach out to us. We have the tools to help you train your team to be vigilant against hackers. We want you as safe as possible!

Information courtesy of:
https://www.proofpoint.com/us/resources/threat-reports/state-of-phish
https://www.cisa.gov/shields-up https://www.knowbe4.com/free-it-security-tools

We turned 15! On March 6, 2022

EMPLOYEE SPOTLIGHT

Cameron Campbell

Cameron has just celebrated two years of working at ITS. He joined us in January of 2020. In his short time here, Cameron was promoted from Technical Support Engineer to Technical Support Manager, overseeing a team of six technicians.

During this time, he earned IT Certifications; graduated from Colorado Mesa University with a Bachelor of Science degree in Computer Information Systems; married his wife, Jordan; and is now assistant coaching the Palisade High School Varsity Baseball Team!

Never one to rest on his laurels, Cameron is currently studying for his Project Management Certificate through Google.

In his spare time (if he has any), you may see him out on the golf course playing a competitive round against our owner, Ryan, or boasting about his beloved Kansas City Chiefs!