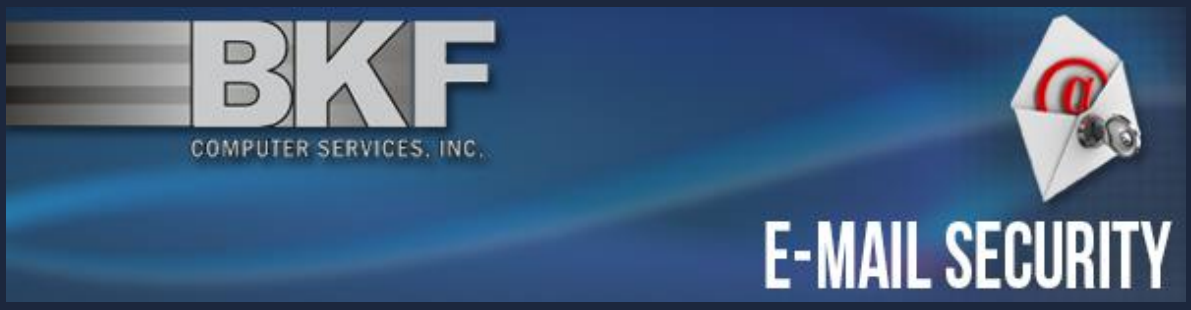
Proofreading Sample
BKF Computer Services
20 Errors Fixed



BKF Computer Services, Inc.

March 19 2021

Dear Brian,

In this final installment of our three part newsletter series on security we will be discussing E-mail Security. If you missed our previous two newsletters they can be viewed on our website. Part one discussed *Social Media Security* and part two discussed *Basic Computer Security*.

Importance of E-mail Security

E-mail is used every day, almost constantly in both personal and business communication. It is fast, easy, and incredibly convenient. However, if you are not aware of all the dangers that can come from using e-mail improperly or without regard to security it can become a huge headache! In this newsletter we hope to enlighten you with some useful advice and tips on how to stay secure when using e-mail.

E-mail Security Tips

- Never respond to e-mails that request financial information. Always be suspicious of an e-mail that requests account information such as a password or username and includes a "link" for you to enter it. No reputable service will EVER ask you for this information through e-mail.
- Avoid being "Phished". Phishing e-mails use generic greetings such as "Dear valued customer" since they will not have access to your real name because they are spam. They also tend to make alarming claims such as your account details have been stolen.

In This Issue

Social Media

Like us on Facebook
BKF has a brand new Facebook fan page. Keep in touch with us and let us know how we are doing!

Follow us on Twitter
BKF is also on Twitter! Engage in some conversation and keep up-to-date on what is happening by following us @bkfcomputers.

Connect on LinkedIn
Connect with us on LinkedIn and help us promote our services while expanding your footprint in the professional world!

Join Our Mailing List!

mails. The links may take you to a site that looks legitimate but in reality it is a bogus site used to steal your information.

- Regularly check your bank and financial statements by manually going to their website and logging in. Do not log-in through any e-mails.
- Ensure the website you are visiting is secure. A secure website will start with "https://" rather than "http://". The "S" means it is a server using encryption. This doesn't always mean the website is legitimate though, so use your best judgement and always error on the side of safety.
- Never open or reply to spam e-mails. This will verify to the sender that your e-mail is valid. Rather, immediately filter your spam into the "spam" folder in your e-mail client.
- Always report suspicious activity. If you receive a suspicious e-mail, forward it to your email client to verify it is safe. Many companies have a dedicated e-mail address for reporting suspicious e-mail activity.
- Only accept/download attachments that you have requested, or you know are legitimate. It also never hurts to scan the files with your anti-virus software prior to opening them. You can set your anti-virus software to do this automatically. .

More on "Phishing"

If you haven't heard of "phishing" e-mails don't fret, we are here to explain them a little more for you. Essentially, a "phishing" e-mail is one sent out by someone who is attempting to obtain personal information about you. These e-mails are often quite malicious in nature because they disguise themselves as if they were common institutions such as banks, credit unions, and popular online vendors, etc.

The e-mail will likely start with a generic greeting with no personalization to it. This is because the sender doesn't currently have any of your personal information. The e-mail will often have a misspelling such as "1nformati0n" to by-pass any anti-spam software.

Typically, the e-mail will say something like "your account information has been compromised" and will likely ask you to a click on a link and enter your information so you can "secure" your account. This link will take you to a bogus website that might look exactly like the real website. Once you reach this page it could already be too late. If you enter any information on that page it will likely be sent to the original sender and then they will have access to your real account.

In Conclusion

By following the guidelines in this newsletter and using your

best judgement you should be much safer while using e-mail. The internet can be a great resource but if you are not informed of all the risks it can also be a dangerous place. Remember to always error on the side of caution, especially when dealing with any personal or financial information.

We hope that these newsletters have been helpful in keeping yourself and your family more secure. Should you ever have any questions or concerns on how to protect your social media profiles, computers or email please contact us!

BKF is grateful for all of the support of our loyal customers and is always striving to provide the best service for you. Let us know how we can improve your customer experience by sending us feedback, giving us a call or referring us to your friends and business associates for their next IT project!

Sincerely,

Brian Fischer and The BKF Team
BKF Computer Services, Inc.

BKF Computer Services, Inc | 708-562-6819 | ineedhelp@bkfcomputers | http://www.bkfcomputers.com
2205 S. Wolf Road - Suite 300
Hillside, IL 60162

Visit our website | www.bkfcomputers.com