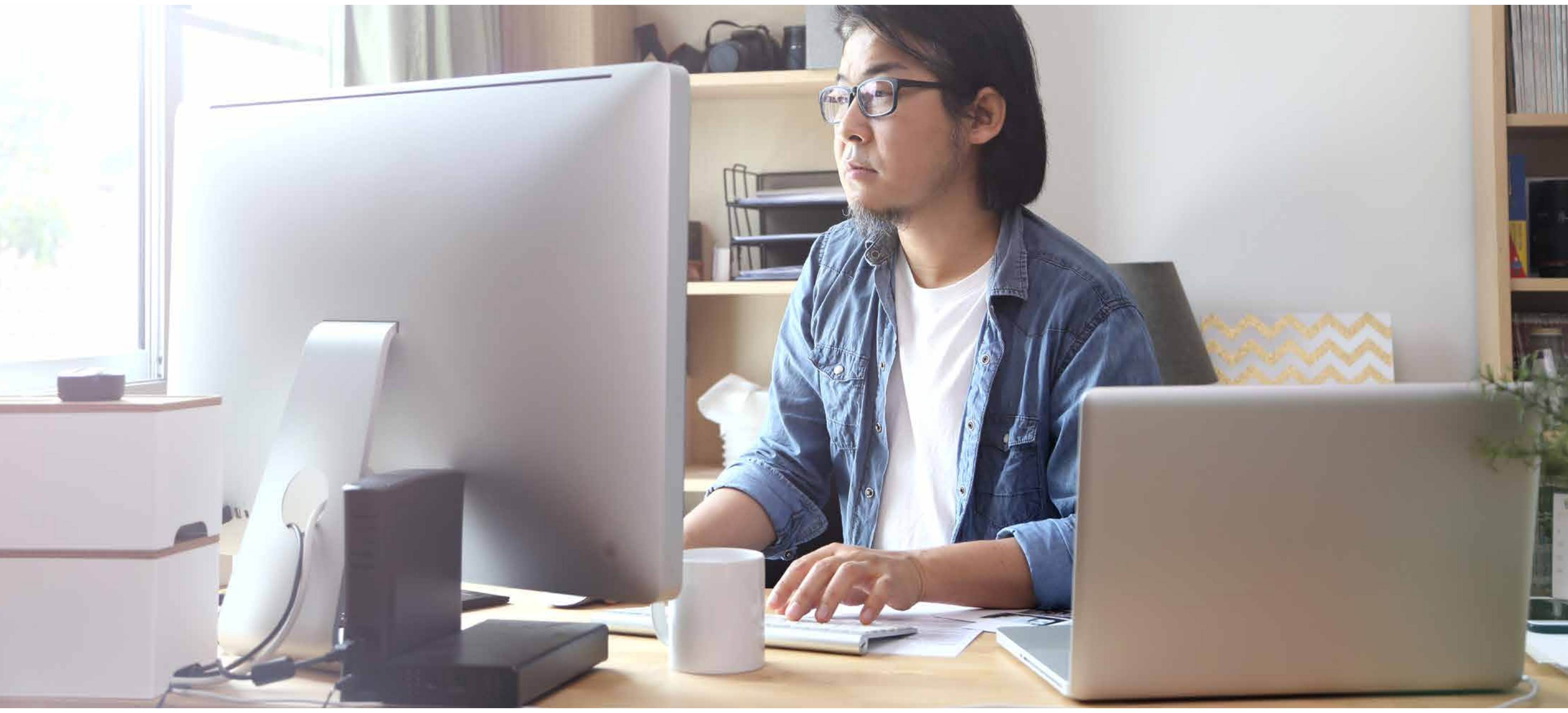
The Online Frontline | Vol.03

First Data is now fiserv.



Six tips to help your employees avoid falling hook, line and sinker to phishing scams

Hackers are taking advantage of the COVID-19 situation by casting a wider net and trying to instill fear – all with the aim of accessing your employees' personal and financial data. And since so many of us are working from home, falling into their trap could put company and customer information at risk..

Help your employees practice safe clicking by passing on these six tips to avoid being phished:

Check the link or email address

Encourage employees to hover their mouse over email links to see where the URL leads to.

Don't take the urgency bait

Let staff know to be wary of any email that insists on acting urgently.

Ignore requests for personal information

Legitimate organizations, including an employer, would not request personal information to be shared online.

Suspect bad grammar, punctuation and misspellings

Spelling errors and bad grammar often point to a scam. Provide your staff with examples of sentences to watch out for.

Skip messages with generic greetings

When an email starts with "Dear Madam" or "Dear Sir," proceed with caution.

Keep browsers up to date

Ensure your staff members download and install updates to shut down loopholes hackers have discovered.

Conclusion

Visit FirstData.com/Security and please contact your Fiserv Relationship Manager today for more information.

FirstData.com