A10: Email Security

Michael Petranick  
Bellevue University  
CYBR 250: Intro to Cyber Threats

Email Security

In 2020, it is hard to do anything without email. It is a part of everyday life. New employees are given a work email when they start, email is required to create a new account on a social media site, and billing statements are mostly paperless, requiring an email address to receive them. Email may have been a luxury 25 years ago, but they have become just as important as a physical address. Most email services are free, and business emails come with cost. As important as email is, it comes with many benefits, but just as many risks, whether someone gets access to your personal information, or having potentially drastic effects on a national election.

Some of the top free email services in the world include Google, Yahoo!, Outlook (formerly Hotmail), and iCloud. Within a few minutes, a user can create an email account, opening the user up to increased access to websites. In some cases, a user cannot access a social media site unless he/she has an account, and an account requires an email address. If Amazon is out of stock on a product, a user can enter his/her email address to receive an email update when the product is back in stock. Email works a lot faster than regular mail. Mail can take days to send while email is sent in a matter of seconds, prompting a faster reply. While email has a lot of benefits, it does come with some risk.

Any activity on the internet comes with certain level of risk. Free email is no exception. Leo Notenboom, a former software developer for Microsoft, states, “I can easily identify the single biggest risk for anyone using free email in any way, at any time, and for any reason: lack of customer support. THERE IS NONE.” (Notenboom, 2018). Notenboom explains that no one is available to help a user experiencing a problem with email, whether it involves losing an email or access to an account. Notenboom states that while free email is advertised as free, it does come with cost. Email is supported by advertising. Seeing ads along the sides of your web page is very common. Notenboom also raises the concern of privacy. “Advertising based on the contents of email raises the issue of privacy; it ‘reads’ your email to determine which ads to display. Some services may also use your information to target ads elsewhere, tailor features and functionality based on your usage, or even share your information – presumably anonymized – with third parties.” (Notenboom, 2018). Spam is another “cost” with free email. Most free email services come with a lot of spam emails, and legitimate email can be lost in all the spam messages. Finally, with spam messages, a user is prone to scams and phishing attacks. Phishing attacks are emails posing as legitimate websites or sources asking for personal information such as social security numbers, bank and credit card information, that a cybercriminal can steal. Phishing has affected anyone with personal and business emails. In 2020, cybercriminals used the presidential election to target unknowing victims.

In October 2020, one month before the general election, it was discovered that cybercriminals were using email to send scams to residents in Arizona claiming to be from the United States Election Assistance Commission stating there is an issue with a user’s account. If the user clicked on the link supplied in the email, the user was taken to a page designed to look like an Arizona government page. “The link in the email sends users to a web page that spoofs ServiceArizona -- part of the state government of Arizona -- complete with images pulled directly from the state's official site.” (Howes, 2020). It was discovered that the email was sent through SendGrid, which recently had a problem with compromised accounts. In August 2020, it was reported, “Sendgrid is grappling with an unusually large number of customer accounts whose passwords have been cracked, sold to spammers, and abused for sending phishing and email malware attacks.” (Krebs, 2020). The information requested on the fake ServiceArizona site included the user’s name, date of birth, social security number, and driver’s license information. Internet security company KnowBe4 theorizes the intent was identity theft. It is unclear if the information was to be used to affect the election in any way. Hours after KnowBe4 accessed the site, the site was shut down.

In conclusion, email is a free service that is widely used throughout the internet and a part of daily life, whether for personal or business reasons. While it is free of charge, there are many benefits and risks that come with it. Phishing scams are a threat to inexperienced persons, as it can lead to identity and monetary theft. It is wise to be educated in these types of scams, and to also be aware of the risks living in the digital age.

References

1. Notenboom, L. (2018, October 19). Are Free Email Services Worth It? Retrieved November 10, 2020, from <https://askleo.com/are_free_email_services_worth_it/>
2. Howes, E. (2020, October 2). Malicious Actors Crash U.S. Election: Spoofed Emails Attempt to Gather U.S. Voter Registration Data. Retrieved November 10, 2020, from <https://blog.knowbe4.com/malicious-actors-crash-u.s.-election-spoofed-emails-attempt-to-gather-u.s.-voter-registration-data>
3. Krebs, B. (2020, August 28). Sendgrid Under Siege from Hacked Accounts. Retrieved November 10, 2020, from <https://krebsonsecurity.com/2020/08/sendgrid-under-siege-from-hacked-accounts/>