Avoid The Most Common Email Mistakes

Email is still one of the primary ways we communicate, both in our personal and professional lives. However, quite often we can be our own worst enemy when using email. Here are the most common mistakes people make with email and how to avoid them.

Auto Complete

Auto-complete is a common feature in most email clients. As you type the name of the person you want to email, your email software automatically selects their email address for you. This way you do not have to remember the email address of all your contacts, just their names. The problem is when you know people that share similar names, it is very easy for auto-complete to select the wrong email address for you. For example, you may intend to send a very sensitive work email to "Janet Roberts", your co-worker, but instead auto-complete selects the email address for "Janice Rodriguez", your child's basketball coach. You end up sending a sensitive work email to someone you barely know. Always double check the name and the email address in any sensitive email *before* you hit send. Another option is add the recipient's email *after* you have drafted your message, ensuring you selected the intended individual.

Reply-All

In addition to the "To" field when you create an email you also have a "CC:" option. "CC:" stands for "Carbon Copy", which allows you to copy additional people on your email and keep them informed. When someone else sends you an email and has CC'ed people on the email, you have to decide how you want to reply: just to the sender or to everyone that was included on the email via Reply-All. If your reply is sensitive, you most likely want to reply only to the sender. However, be careful as it's very easy to mistakenly hit "Reply-All," which means you would reply to everyone on the email. Once again, whenever replying to a sensitive email, always double check who you are sending the email to *before* you hit send.

Emotion

Never send an email when you are emotionally upset--it could harm you in the future, perhaps even costing you a friendship or a job. Instead, take a moment and calmly organize your thoughts. If you need to vent your frustration, open up a new email (make sure there is no name or email address in the TO section) and type exactly what you feel like saying. Then get up and walk away from your computer, perhaps make yourself a cup of coffee or go for a walk.

When you come back, delete the message and start over again. It may even help to have a friend or co-worker review your draft response objectively before you send it. Or better yet perhaps once you have calmed down, pick up the phone and simply talk to the person, or speak face to face if possible. It can be difficult for people to determine your intent with just an email, so your message may sound better on the phone or in person. Remember, once you send that email, it exists forever.

Privacy

Finally, email has few privacy protections. Your email can be read by anyone who gains access to it, similar to a postcard sent in the mail. Your email can easily be forwarded to others, posted on public forums, released due to a court order, or distributed after a server was hacked. If you have something truly private to say to someone, pick up the phone and call them. If you are using your work computer for sending email, remember that your employer may have the right to monitor and perhaps even read your email when using work resources.

Attachments

If you're attaching documents to your message, double-check that you've attached the correct versions of the correct files before sending.

Guest Editor

Steffanie AK Schilling is a cybersecurity rockstar, having her roots in the social sciences. Honored as an "Innovator and Difference Maker in Cyber", she is an inaugural member of ShareTheMicInCyber and currently serves as the youngest ever VP of Infragard - Northern Ohio. She is a highly requested speaker on Diversity, Equity, Inclusion, Justice, and Security Education and Awareness. (https://www.linkedin.com/in/steffanieschilling/).

Resources

Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Identity Theft: https://www.sans.org/newsletters/ouch/identify-theft/
A Career in Cybersecurity: https://www.sans.org/newsletters/ouch/a-career-in-cybersecurity/