TTECtrust

Our commitment to you!

Don’t Let the CyberGrinch Steal Your Holiday (or personal info)

The holidays are a great time for giving your friends and family that perfect gift you hunted for in stores and on the Web. Unfortunately, they’re also a great time for giving cybercriminals the perfect gift, too—your personal data—that you didn’t even mean to give them!

During the holidays, many of us spend more time shopping on the Internet and, preoccupied with all there is to do, less time paying attention to “phishy” emails. Both habits can be dangerous. While occasional, limited personal use of your work computer is allowed, please be aware that checking your personal email online for holiday shipping information may leave us vulnerable to phishing attempts.

This season don’t let the CyberGrinch sneak into your cyber home (or TTEC’s) and steal your holiday cheer. Be aware of, and take precautions to avoid, these common holiday scams:

- Shopping Scams
- Order/Shipping Notification Scams
- Gift Card Scams (targeted to employees)
- Charity Scams

Learn more about each scam and how to avoid it...

Data Security

Why USB drives are taboo at TTEC

Did you know that using a USB drive (aka thumb drive or flash drive) could potentially infect not just your own computer but TTEC's entire network? "How?" you ask. (Hey, thanks for asking.)

Visit the Mosiac space for details!

Working Remotely from Other Countries

As you know, you need to be extra careful when you're working remotely. That includes avoiding public WiFi, securing your machine and using a privacy filter.

Please also remember that **employees shouldn't work remotely from China, Russia, Iran and North Korea** given increased security risks.

Online Awareness

What is the Internet of Things and how does it affect TTEC?

The "Internet of Things" (IoT) sounds a lot more complicated than it really is. If you break it down, "things" are physical objects that wouldn't normally be connected to the Internet, like watches and thermostats.

The "Internet of" refers to connecting these physical things to the Internet, enabling them, through sensors, to send and receive data and communicate information—all without human interaction.

Learn more...

Asset Protection

Sometimes not sharing is good

Remember what your mama taught you about sharing? Well, forget it all—at least when it comes to your personal information. This includes information from log-in credentials and passwords to your social security number and date of birth.

Passwords that fall into the wrong hands, for instance can result in a ransomware attack, data breach or TTEC being found out of compliance because unauthorized parties viewed protected data. Personal information that falls into the wrong hands, like your social security or credit card number, can lead to financial loss.

You have control over what personal information you share on purpose, visit Mosaic for tips for not sharing it by accident:

Learn more...

Click here to visit the TTEC Trust Mosaic space for more details.

The "Learn more" link in the intro "Don't Let the CyberGrinch Steal your Holiday" takes the reader to the following copy on TTEC's Intranet platform:

Shopping Scams: Because cybercriminals know people are shopping even more over the holidays, they use that knowledge to their advantage by offering holiday "deals." Counterfeit holiday promotions could come through emails in which hackers pose as well-known retailers such as Target and online brands such as Amazon, offering fake deals to get you to click on a malicious link. You could also find these supposed deals through fake websites that you discover while surfing the web. Scammers particularly prey on bargain hunters around Black Friday and Cyber Monday. Remember, if a deal looks too good to be true, it probably is.

> **To avoid this scam**: Only shop from websites and brands that you trust and go directly to their website. If you find somewhere new you'd like to order from, research it online first to make sure it's reputable. If you receive an email from a trusted brand that seems too good to be true, review these phishing tips first.

Order/Shipping Notification Scams: Cybercriminals are aware that people order so much stuff over the holidays they sometimes don't remember what they ordered or from whom, so they send out phishing emails. The email could be about a fake order, asking you to review the order. Or it could be a shipment confirmation or shipping update from well-known couriers like Amazon, FedEx and UPS. The goal, of course, is to get you to click on a malicious link or to provide personal information.

> **To avoid this scam**: If you receive an order or shipping confirmation/update email you didn't expect, find another way to assess the request. For example, go to the brand's website and visit your account to check on your recent orders. If you are told your account will be charged for something you absolutely know you didn't buy, it is most likely another type of scam. The CyberGrinch is hoping your concern about being charged will cause you to click on the link. Don't fall for it!

Gift Card Scams (targeted to employees)
Criminals often send victims fake coupons and gift cards to try to get them to provide their personal information. Now, they have an even more sophisticated gift card scam up their sleeves that specifically targets employees. After researching a company to get an idea of their internal hierarchy, a cybercriminal will pretend to be someone senior in the organization and send an email to an employee at a lower level requesting they purchase gift cards and send the codes over email. The request is usually urgent, such as for a client meeting that afternoon.

> **To avoid this scam**: If you receive an email from your manager with an urgent or unusual request, such as a request to buy multiple gift cards, find another way to assess the request before you act. For example, send your manager an email or a message on Teams or, better yet, talk to him or her on the phone/in person to confirm the request is authentic

Charity Scams: During the holidays, people tend to be in a giving mood and thus are more likely to donate to a charity during this time. Cybercriminals know this and devise ways to have you (mistakenly) donate your hard-earned money to them instead. They do this by sending an email (or calling) posing as a member of a charity organization that doesn't exist. Or they mimic a well-known charity's

communications and website and ask you to click on a link to donate (and provide your financial information).

To avoid this scam: Prior to donating to an unknown charity, verify that they have a valid Taxpayer Identification number by visiting their website or calling the charity directly. You can also verify a charity by contacting organizations like Charity Navigator or CharityWatch. To avoid donating to fake charities that might be mimicking real charities, see these phishing tips first. (link)